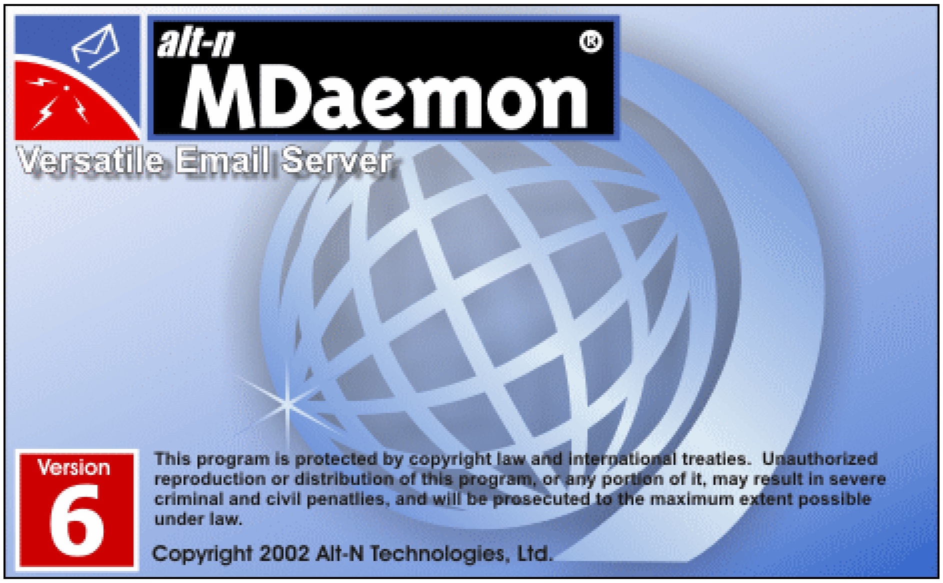


User Manual

ALT-N TECHNOLOGIES, LTD.

MDaemon® Version 6 – User Manual

MDaemon is a product of Alt-N Technologies.
1179 Corporate Drive West, Suite 103
Arlington, Texas 76006
817.652.0204
Fax: 817.652.0590
www.mdaemon.com

LICENSE AGREEMENT

Please read this entire agreement. If you do not agree to the terms of this agreement promptly return your distribution materials to the place you obtained them for a full refund or delete your trial package.

ALT-N TECHNOLOGIES END-USER LICENSE AGREEMENT

This End-User License Agreement ("EULA") is a legal agreement between you ("Customer" or "Sub Licensee") and Alt-N Technologies ("Licensee") for the Alt-N software product(s) you are installing which include(s) computer software, "online" or electronic documentation, and may include associated media and printed materials ("SOFTWARE PRODUCT" or "SOFTWARE").

By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, promptly return the entire unused SOFTWARE PRODUCT, including all subscription UPDATES that you may have received as part of the SOFTWARE PRODUCT, to the place from which you obtained it for a full refund and/or delete all files related to your trial demonstration version of the SOFTWARE PRODUCT.

ALT-N TECHNOLOGIES SOFTWARE LICENSE

This SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold. The SOFTWARE PRODUCT consists of product documentation, a server application, and support files individually identified as "COMPONENT" and collectively referred to herein as "SOFTWARE".

GRANT OF LICENSE.

Alt-N Technologies grants to you as an individual, a personal, non-exclusive, non-transferable license to install and execute a single instance of the SOFTWARE on a single computer or on multiple computers provided that there is no chance of concurrently running two or more distinct instances of the SOFTWARE simultaneously for the purposes of evaluating the performance of the SOFTWARE PRODUCT for a period of no more than 30 days. If after that time continued use of the SOFTWARE PRODUCT is desired then the SOFTWARE PRODUCT must be registered with Alt-N Technologies subject to the terms as laid out in the registration information which can be found in the documentation accompanying the SOFTWARE PRODUCT. If you are an entity Alt-N Technologies grants you the right to appoint an individual within your organization to use and administer the SOFTWARE subject to the same restrictions enforced on individual users.

COPYRIGHT

All title and copyrights in and to the SOFTWARE PRODUCT are owned by Alt-N Technologies, its suppliers, or component vendors. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may either (a) make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes, or (b) install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

THIRD PARTY COMPONENT LICENSING TERMS

Third party utilities, application programs, and/or components designed to integrate with the SOFTWARE PRODUCT are subject to the license terms governing those products.

You may not reverse-engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law, notwithstanding this limitation.

DISCLAIMER OF WARRANTY

NO WARRANTIES. THE SOFTWARE PRODUCT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALT-N TECHNOLOGIES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST INFRINGEMENT, WITH REGARD TO THE SOFTWARE PRODUCT. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS WHICH VARY FROM STATE TO STATE.

CUSTOMER REMEDIES.

ALT-N TECHNOLOGIES ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY SHALL NOT EXCEED THE PRICE PAID FOR THE SOFTWARE. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ALT-N TECHNOLOGIES BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE PRODUCT, EVEN IF ALT-N TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Chapter List

Table of Contents

Section I – MDaemon's Primary Features

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 9

CHAPTER 25

CHAPTER 26

CHAPTER 27

CHAPTER 28

APPENDICES

SECTION I

MDAEMON® VERSION 6.0.3

MDaemon's Primary Features

Chapter

1

MDaemon® v6.0

Versatile Email Server for Windows

Introduction

MDaemon Server v6 brings SMTP/POP/IMAP and MIME mail services commonplace on UNIX hosts and the Internet to Windows based servers and microcomputers. MDaemon is designed to manage the email needs of any number of individual users and comes complete with a powerful set of integrated tools for managing mail accounts and message formats. MDaemon offers a scalable SMTP, POP3, and IMAP4 mail server complete with LDAP support, an integrated browser-based email client, content filtering, spam blockers, extensive security features, and more.

MDaemon Standard and Pro

Alt-N Technologies' MDaemon Server is available in two versions: MDaemon Standard and MDaemon Pro. With the powerful features of MDaemon Standard, you can collect your network's email from a single ISP provided POP3 account, or host an entire domain with MDaemon's full-fledged SMTP server. With the increased functionality of IMAP4 and Multiple Domain Support, MDaemon Pro is an ideal email backbone for enterprise level organizations. MDaemon Pro also adds group calendar and scheduling, an instant messaging system, multiple language support for WorldClient, automatic domain gateway creation, and more to MDaemon Standard's already extensive set of features. For a complete discussion on the differences between MDaemon Standard and Pro see the white paper, "*MDaemon Versions: Comparing Standard and Pro*". This white paper and other helpful resources can be obtained form our web site at www.altn.com.

MDaemon Features

MDaemon is equipped with many features besides SMTP, POP, and IMAP email processing. The following is a list of just some of those features.

- MDaemon's extensive parsing features make it possible to provide email for an entire LAN with as little as a single dial-up ISP POP3 mailbox. This makes it possible to provide email to an entire network for a fraction of the normally associated cost.
- MDaemon Server v6 features a complete suite of Mailing List or email group management functions allowing for the formation of an unlimited number of distinct distribution lists that can contain local and/or remote members. Lists can be set to allow or refuse subscription requests, be public or private, post replies to either the list or the originator of the message, be sent in digest format, and be configured using numerous other features.

- An integrated component of MDaemon is WorldClient. This exciting product makes it possible for your users to access their email using their favorite web browser rather than from a workstation dependent email client. This tool is perfect for mobile staff and users who do not have a dedicated machine from which to access their email.

- WorldClient is equipped with a complete suite of email client features. Send and receive email, spell check messages, manage your email in multiple personal folders, display the interface in any of 18 languages, schedule meetings and appointments with group Calendar & Scheduling features, manage your MDaemon account settings (when used in conjunction with WebAdmin), manage contacts, and more. WorldClient is also equipped with ComAgent, a small utility that can be downloaded and installed on a user's local computer. This provides easy access to your email and folders and checks for new messages without having to open your web browser. It also includes a complete Instant Messaging system that can be used to quickly "chat" with other MDaemon/WorldClient users.

- MDaemon is equipped with many features designed to help you make your email system secure. The Spam Blocker feature will help you put an end to most "spam" email messages that "spammers" try to route through or to your domain. IP and Host Screening and Address Suppression provide the capability to screen and prevent certain addresses and domains from connecting to or sending mail through your system. They also make it possible to connect to specific IP addresses while screening all others.

- Equipped with support for Lightweight Directory Access Protocol (LDAP), MDaemon can keep your LDAP server up to date on all of its user accounts. This makes it possible for users with mail clients that support LDAP to "share" a global address book that will contain entries for all of your MDaemon users as well as any other contacts that you include. You can also choose to use your LDAP server as the MDaemon user database instead of its local `USERLIST.DAT` system. Thus, you can configure multiple MDaemon's at different locations to share the same user database.

- MDaemon can be configured to keep your Windows Address Book or Microsoft Outlook Contact Store up to date with your user information. This provides another means of making a global address book available to your users.

- Address Aliases provides the ability to route email messages addressed to "fictitious" mailboxes to a valid account or mailing list. This makes it possible for individual accounts and lists to have "multiple" email addresses at one or more domains.

- The Domain Gateways feature provides the option of setting up separate domains for various departments or groups that may be local to your network or located somewhere else on the Internet. Using this feature, all mail addressed to a domain for which MDaemon is acting as a gateway will be placed in that domain's mailbox by MDaemon. It can then be collected by that domain's MDaemon server or email client and distributed to the domain's users.

- Accounts can be controlled remotely by users by using specially formatted email messages. This allows greater administrative flexibility, and empowers users by turning day-to-day simple account maintenance tasks, such as changing passwords, over to them.

- Support for WebAdmin. This is a free web-based remote administration application that can be obtained from www.altn.com. It integrates perfectly with MDaemon and WorldClient and enables your users to review and edit their account settings via their web-browser. You can designate which settings that your users may edit, and assign access permissions on a per account basis. WebAdmin can also be used by the Administrator (and whomever else you wish to allow) to review or edit any of MDaemon's settings and any other files that you wish to make available to the WebAdmin system for reviewing.

- Included with MDaemon is the MDConfig Remote Configuration Client. This utility makes it possible for a Network Administrator or Supervisor to access and change any of MDaemon's settings from a remote location by easily installing it on a remote machine. Moreover, because its interface is virtually identical to MDaemon's, you won't have to familiarize yourself with a new set of controls.

- With File Catalogs, the email administrator can create password protected groups of files which users can have encoded and automatically sent to them through the use of specially formatted email messages.

- Account mailbox formats can be abstracted using Mailbox Format Files (MBF), which allows for a wide range of mail system compatibility.
- An internal message transport system known as RAW mail provides a simple method for placing messages into the mail stream and greatly simplifies custom mail software development. Using RAW, a complete mail system can be devised using a simple text editor and a couple of batch files.
- A highly versatile Content Filtering system makes it possible for you to customize server behavior based on the content of incoming and outgoing email messages. You can insert and delete message headers, add footers to messages, remove attachments, route copies to other users, cause an instant message to be sent to someone, run other programs, and more.
- Complete support for virus scanning and protection through MDaemon AntiVirus. This utility provides potent anti-virus protection. Messages can be scanned for viruses and cleaned or deleted automatically before ever reaching the intended recipients. Further, you can configure MDaemon to send a message to the administrator, sender, and recipient of the infected message notifying them of the virus. MDaemon AntiVirus can be obtained from www.altn.com.

What's New in MDaemon Version 6?

Expanded and Improved WorldClient

New WorldClient Themes

We've added two new themes to WorldClient: "LookOut" and "Simple".

LookOut requires Internet Explorer 5.5 or higher, and it has a "look and feel" similar to Microsoft Outlook Express.

"Simple" is designed to be very basic and fast in order to accommodate slow Internet connections. It doesn't use frames and contains a greatly limited number of graphics.

Shared Calendaring and Scheduling

WorldClient has been enhanced with a complete calendar system for scheduling meetings and appointments, and for creating global and personal memos. You can schedule meetings and designate attendees (causing an email notification to be sent to each person), schedule appointments for yourself, create global and personal memos, and even import and export to Microsoft Outlook and other iCalendar compliant email programs. Additionally, you can set permissions for your calendar and thus control the level of access that others will have to it (i.e. whether they can see or create events on your calendar). You can also view or modify the calendars of other WorldClient users based upon the permissions that they have set. Finally, when used with ComAgent, you can receive instant messages each time your calendar is modified and when reminders about approaching calendar events are needed.

For more information, see *Calendar & Scheduling System*—page 74.

Improved Email Features

WorldClient now behaves more like a traditional IMAP client. You have the option to flag messages as deleted or undeleted instead of using a "trash" or "deleted items" folder like in POP clients (although the "trash" method is still available if that is your preference). Further, you can now select which IMAP folders you wish to subscribe to and which ones to hide. Finally, the folders WorldClient uses for Drafts, Sent, and Trash can be selected and renamed instead of being forced to use specific "system" folders.

When used in conjunction with WebAdmin—Alt-N's free remote server administration application—WorldClient has been further enhanced to allow you to collect email from multiple mail sources and deposit it into your WorldClient folders. WorldClient does this by interacting with MDaemon's MultiPOP system and then utilizing your IMAP Filters. Your MultiPOP and IMAP Filters are reached from within WorldClient by clicking "MDaemon Settings" on the Options page. This link launches WebAdmin in a separate browser window from which you can modify your settings. In this way, control is given to users while still being policed by the MDaemon administrator.

All of these new capabilities can be configured by individual users via various controls on the Personalize, Folders, and MDaemon Settings pages within WorldClient Options. They can also be configured globally and per-domain like all other user settings in the `Domains.ini` file. The keys of interest are:

```
[Default:UserDefaults]
HideUnsubscribedFolders=No
UseIMAPDelete=No
DraftsFolderName=Drafts
SentFolderName=Sent
TrashFolderName=Trash
```

Run WorldClient under IIS

WorldClient is equipped with a built-in web server and therefore doesn't require Internet Information Server (IIS) to operate. However, to accommodate those who wish to use IIS, support has been added to MDaemon 6.0 thus making it possible for WorldClient to function as an ISAPI DLL.

For more information, see *Running WorldClient under IIS*—page 80.

ComAgent

Replacing WCWatch in MDaemon 6.0 is ComAgent, a secure instant messaging system, address book client, and tray applet that provides address book synchronization and quick access to WorldClient's email features. ComAgent can be downloaded by each WorldClient user and then installed on the individual's local computer. It is preconfigured for the specific user when downloaded thus limiting the need to configure it manually.

For more information, see *ComAgent*—page 75.

Automatic Address Book Synchronization

By using ComAgent in conjunction with Alt-N's LDaemon LDAP server (v2.0 or later) to maintain WorldClient's Public and Private address books, you can provide two-way synchronization between LDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

MDaemon can maintain an accurate and continuously up to date LDAP database of users by communicating with LDaemon each time an MDaemon account is added, removed, or modified (see

LDAP Options—Page 94 for more information). ComAgent has the ability to poll LDaemon at regular intervals and acquire all the contact information being stored there. It then publishes this information to the local computer's Windows Address Book or contact store. This has the effect of instantaneously updating any local software package which uses the local address book system (for example, Outlook/Outlook Express).

For more information on this feature and other Address Book related features in MDaemon and WorldClient, see:

Automatic Address Book Synchronization—Page 87

LDAP Options—Page 94

Miscellaneous Options | WAB—Page 209

Secure Accountable Instant Messaging System

ComAgent is equipped with a simple but effective instant messaging (IM) system. With this system you can communicate instantly with any other account on your MDaemon server. You can choose a list of "buddies" from a list of all MDaemon users and then see which ones are online and ready to receive an IM. You will also be able to start a group conversation involving several buddies at once. All of the IM features are available via the shortcut (right-click) menu within ComAgent.

Because many businesses and administrators have reservations about using an Instant Messaging system in their company due to the inherent lack of centralized accountability and the inability to monitor IM traffic in traditional and well known IM clients, we have designed ComAgent's instant messaging system to minimize those deficiencies. First of all, our system is not peer-to-peer—individual ComAgent clients do not connect directly to each other. Further, because every IM passes through the server, each message is logged in a central location accessible to the MDaemon/WorldClient administrator. Thus a record of all conversations can be maintained for the security of both your company and your employees or users. IM activity is logged in a file called `InstantMessaging.log` located in the `MDaemon\LOGS\` directory. The assurance of accountability is also the primary reason we do not support other IM clients such as ICQ, AOL, and MSN. We may, however, add that capability as an optional feature in some future version of MDaemon. Finally, our IM system is secure in that each transaction is strongly encrypted from start to finish so that plain text is never transmitted.

For more information see, *ComAgent's Instant Messaging System*—page 76.

WebAdmin Integration

Support for Alt-N's next generation of web-based configuration tools has been fully integrated into MDaemon. WebConfig has been removed from MDaemon 6.0 and now WebAdmin is the browser-based tool of choice for remote server administration. Though not included in the MDaemon installer, WebAdmin is provided as a separate free download. You can WebAdmin from Alt-N's web site at `www.altn.com`.

Note: If you are upgrading to MDaemon 6.0 from a previous version then you can safely remove the WebConfig folder from your MDaemon directory structure.

For complete information on WebAdmin see the WebAdmin user manual, which can also be obtained from Alt-N's web site at `www.altn.com`.

Enhanced IMAP Features

Improved IMAP Folder Sharing

MDaemon version 6 supports the sharing of Public and User IMAP Folders. Public folders are extra folders that do not belong to any particular account but can be made available to multiple IMAP users. User folders are IMAP folders that belong to individual MDaemon accounts. Not to be confused with public FTP or html folders, MDaemon's Shared IMAP folders, whether Public or User, may not be accessed by everyone. Each shared folder must have a list of MDaemon users associated with it, and only members of that access list may access it via WorldClient or an IMAP email client.

When IMAP users access their list of personal folders, shared public folders and shared user folders to which they have been given access will also be displayed. In this way certain mail folders can be shared by multiple users but still require each user's individual logon credentials. Furthermore, having access to a folder doesn't necessarily mean having full read/write or administrative access to it. Specific access rights can be granted to individual users, thus allowing you to set different levels of access for each one. For example, you might allow some users to delete messages while restricting that from others.

These access rights are controlled through support for Access Control Lists (ACL) that has been added to MDaemon 6.0. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access rights to your folders to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the MDaemon version 6 interface. Right now very few email clients support ACL directly but there is an excellent utility from www.bynari.net called InsightConnector that will add this functionality (and more) to Microsoft Outlook.

ACL is fully discussed in RFC 2086, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2086.txt
```

For more information, see *Shared IMAP Folders*—page 100.

Public Folder 'Per-user' Flags

IMAP public folders can now store flags (i.e. new/unread/deleted) on a per-user basis. With this option enabled IMAP users will not share the same message flags globally with all other users but will maintain their own message flags independent of other users. These flags are stored under the user's mail directory in the PublicFolderFlags directory.

A new option has been added to the Public Folders dialog which will let you set whether or not the folder should use per-user flags.

For more information, see *Shared IMAP Folders*—page 100.

Support for InsightConnector from Bynari, Inc.

An exciting plug-in from Bynari, Inc called InsightConnector is available for Microsoft Outlook users. This plug-in adds ACL support to Outlooks IMAP capability and also allows you to use MDaemon as a complete replacement for Microsoft Exchange Server. With MDaemon, Outlook, and

InsightConnector you can completely replace Exchange Server with no loss of functionality. Users can share calendars, contacts, to-do lists, and everything else previously only possible with an Outlook/Exchange Server combination.

MDaemon has been enhanced in the following ways to work well with InsightConnector:

1. A new switch added to the Shared IMAP Folders dialog will allow you to configure an alternative to the "/" character that MDaemon uses to delimit IMAP folder strings. For example, if "/" is the delimiter character and "`#Test/Test2`" is specified as a valid IMAP folder, then "`Test2`" will be considered a sub-folder of "`#Test`". This new configuration setting was provided because Bynari's InsightConnector expects a '.' (period) character as the delimiter rather than MDaemon's default "/" character.

2. MDaemon's new ACL support within its IMAP server works well with the ACL support added to Outlook by InsightConnector.

Performance Enhancements

Configuration Caching

MDaemon now uses an in-memory caching system for the settings found in many of the `.ini` and `.dat` files in the `\App\` directory. This system will improve performance considerably but changes made manually or directly to those files while MDaemon is running will not be reflected in the program until MDaemon is restarted or it detects a file called `RELOADCACHE.SEM` in the APP directory.

Smarter 'Smart' Spooling

In the past when a single message was spooled to multiple recipients at the same host MDaemon would abort the entire message transfer if even one of the recipients was refused by the receiving host. This prevented messages from being delivered to valid recipients when a single invalid address was in the delivery list. Although this behavior is technically allowed it is not very efficient. MDaemon has been changed so that this no longer occurs. When MDaemon encounters errors with one or more recipients during message delivery it will continue the delivery process. Afterward, a summary of those recipients which failed will be delivered to the sender of the message.

The smart spooling options will now function in the "*Send every outbound email message to this host*" type of configuration on the Primary Domain Configuration editor (click Setup→Primary domain...→Domain/ISP).

Note

As a result of this change the wording within the `DELERR.DAT` file is no longer appropriate and has been changed. If you are upgrading from a previous version of MDaemon then you should delete your existing `DELERR.DAT` file from the `\APP\` directory and restart MDaemon so that a new one with appropriate wording will be created.

Improved Mailing List /Catalog Control Command Processing

All the Remote Server Control via Email Messages control commands that MDaemon processes for mailing lists and catalogs can now be sent in the message's "Subject:" in addition to the former method of being contained in the message body.

Improved Mailing List Subscribe/Unsubscribe

A system has been added whereby special email addresses will be available for list users to subscribe and unsubscribe easily to your mailing lists. On the Miscellaneous Options dialog you will find a switch that says this:

Honor '<List>-Subscribe' and '<List>-Unsubscribe' addresses

When this switch is enabled MDaemon will always recognize email addresses of this format as valid (as long as the list actually exists). For example: suppose you have a list called `MyList@altn.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@altn.com` and `MyList-Unsubscribe@altn.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@domain.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

Enhanced MultiPOP Collection Options

We've added a new collection method for MultiPOP mail. You can now elect to collect MultiPOP "dynamically". What this means is that MultiPOP mail for a particular user will be collected the next time that user checks his local MDaemon mailbox either via POP, IMAP, or WorldClient. In this way mail is only collected for those users who are checking for it. It's important to note that when a user connects to MDaemon to check for new mail this act **initiates** a MultiPOP collection event. Messages collected by that event will not be available to the user until the **next** time he or she checks for new messages.

In order to further reduce the load that extensive use of MultiPOP can sometimes place on your MDaemon, an option to restrict the number of MultiPOP collections per user per hour has been added to Setup→Miscellaneous Options→MultiPOP. Further, an option to specify a number of minutes to place between back-to-back MultiPOP collection events has also been added.

Additionally, when you specify DomainPOP or MultiPOP hosts to collect mail from you can override the default outbound POP port by appending a new port value to the host name. For example, using "mail.example.com" as a MultiPOP host will connect to that host using the default outbound POP port while using "mail.example.com:523" will connect to that host on port 523.

Ghosts/Terminal Services Support

If you start MDaemon from the command line and pass the `/ghost` command line switch, an engine-less copy of the GUI will start. We call these detached GUIs: ghosts. Since ghosts are detached from the main MDaemon and don't do any mail processing you can usually get better responsiveness out of them. Ghosts use a green tray icon and say "Ghost" in the window caption. You can run a ghost through Terminal Services and edit the properties of the actual MDaemon service. For a ghost to display logging information within the various services tabs you will need to enable the new logging option "*Log each service into a separate log file.*" This option is enabled by default. MDaemon 6.0.0 supports only a single running ghost instance.

Improved Logging

A new switch was added to the Logging Options which will cause MDaemon to maintain separate logs by service rather than a single file. For example, with this switch set MDaemon will log SMTP activity in the `MDaemon-SMTP.log` file and IMAP activity in the `MDaemon-IMAP.log` file. One side effect of these changes is that it is no longer possible to specify an arbitrary file name for the logs so this control has been removed from the Logging Options dialog. Further, a new Spam Blocker log file has been added which will allow you to have an easy reference to the sites that were logged as blacklisted.

Automated Configuration Backup

This new feature makes it possible to archive all MDaemon configuration files at midnight each night. The settings to configure this feature are located on the Disk tab of Miscellaneous Options. You can specify exactly which files and file extensions to back up.

Security Enhancements

Host Screening

Similar to IP Screening, Host Screening allows you to specify the names of remote hosts that MDaemon will or will not accept mail from. When an incoming SMTP connection specifies the name of the remote server in the `EHLO` or `HELO` parameter MDaemon will compare it to the names listed in the Host Screening configuration. If a match is made the session is either allowed or disallowed depending on how you have configured permissions for that particular host.

Enhanced Spam Blocking

Several new options have been added to the Spam Blocker system to further combat unwanted mail. First, a new checkbox is present which will allow you to configure MDaemon to check the IP addresses found in all the "`Received`" headers within SMTP and DomainPOP collected mail. Sometimes spammers will relay spam to you through your ISP. When this occurs the Spam Blocker is fooled because your ISP is usually trusted or is typically not an originator of spam. With this new switch all the IP addresses in the source route of the message will be checked and if any one of them is found to be a known spam source the message will be flagged or otherwise dealt with according to Spam Blocker settings. Additionally, new options have been added which allow you to restrict the depth of this new "`Received`" header processing to only a certain number of headers within each message. One added benefit of this feature is that when you have configure Spam Blocker to process "`Received`" headers within an SMTP delivered email, and then a hit is found, MDaemon can be configured to immediately refuse the email without ever accepting it.

Improved Import/Export Capabilities

When you select the export option and choose a comma delimited format MDaemon will export much more account information now than in previous versions, including forwarding and auto-responder settings.

The import process has been enhanced to accept comma delimited files that contain many more fields than in the past. Each line of the comma delimited text file must contain only a single entry, and the first line must be a base line giving the names and sequence of the fields in subsequent lines. A sample file would look something like this:

```
"Mailbox", "FullName", "MailDir", “AllowAccess”
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"frank", "Frank Thomas", "C:\Mail\Frank\", N
```

For more information on importing accounts from a text file, and for a list of all allowable fields, see Importing Accounts From a Text File—page 249.

Additional Changes

See the `Relnotes.txt` file located in MDaemon's `\Docs\` subdirectory for a complete list of all changes and fixes to MDaemon from previous versions.

Information for those Upgrading from Previous Versions

Version 6 Special Notes

MDaemon is no longer compatible with the original Windows 95 release. MDaemon now requires Windows 95 OSR2 or higher.

Due to complexities added to the Public Folders it will not be possible to administer them via MDConfig in this version.

A new option which is enabled by default requires that messages sent from "Postmaster" take place on an authenticated mail session. This could cause some problems for certain third party software which tries to send messages as "Postmaster". You can disable this switch from within the Alias Editor if is causes you problems.

We changed the name of the WorldClient Watch program to ComAgent in order to better reflect its function both now and into the future. Please direct your WorldClient Watch users to return to their Options page and re-download the installer for ComAgent. After installing ComAgent your users can safely uninstall WorldClient Watch. ComAgent offers some exciting new capabilities.

New Public IMAP Folder functionality does away with the use of mailing lists to govern access to the public folder. Access is now controlled via Access Control Lists. Check each of your public folders to make sure that the upgrade process has set the default permissions and the user permissions correctly.

If you change the LDAP port it will erase your existing LDaemon command line and create a new one reflecting the new port value. Any other command line options you enter will be lost so you need to reenter them each time you change the LDAP port via the GUI (Setup→Primary Domain→Ports tab).

The name of the WorldClient CGI is now "`WorldClient.dll`" instead of "`WorldClient.cgi`". ComAgent will no longer be able to connect to WorldClient with "`WorldClient.cgi`" in the URL, so you will need to change the URL manually or download a new pre-configured ComAgent from WorldClient. If you have created any custom logon pages that post to "`WorldClient.cgi`", change them to use "`WorldClient.dll`".

If you have customized the `RFC822.MBF` mailbox format file you will need to copy `RFC822.MBF` to a different file name and reconfigure your accounts to use the new file. In order to increase performance MDaemon assumes that no modifications to `RFC822.MBF` will ever be made. Messages bound for accounts which are using the `RFC822.MBF` script are simply moved into the users mail directory without being processed through the script processor. The theory is that emails from the Internet are already in RFC822 compatible format. Therefore, processing them through a script designed to translate email into RFC822 format is needless and a great deal of processor power can be conserved by skipping this needless step. However, if the "*Strip X-Headers from local messages*" checkbox is enabled then MDaemon has no choice but to send all the messages through the script processor. So, enable that switch only if you need it.

The MDUSERDLL_EDITLOCALONLY bit mask in the API was changed to more accurately reflect its function. It is now MDUSERDLL_EDITMAILRESTRICTIONS. Also, the MD_SetEditLocalOnly and MD_GetEditLocalOnly functions in the API were changed to MD_SetEditMailRestrictions and MD_GetEditMailRestrictions to more accurately reflect their function. These changes may cause you to need to recompile your custom software applications.

The MD_GetDBPath function has changed in the API/COM object. It now returns void instead of bool. This may require you to alter any applications you have written which uses this function.

Version 5 Special Notes

In order to reduce the size of the installer, the MDaemon User Manual is no longer included. The manual and other documentation is now available for download at:

http://www.altn.com/Documentation

Because ORBS is out of business, and because MAPS/RBL/DUL/RSS have moved to a fee-based structure, the Spam Blocker has been reconfigured with a new set of default hosts. If you'd like to use the new set of hosts you will need to delete SPAMBLCK.DAT from the "...MDaemon\APP\" directory and restart MDaemon.

Due to the expansion of WorldClient's capabilities in MDaemon version 5, an importing program will run during installation that will identify previous versions of WorldClient and ask you if you wish to migrate existing messages from the older version. If this tool does not run during installation, you can execute it manually by running WCIMPORT.EXE from the "...MDaemon\APP\" directory. When importing from WorldClient Pro, only WorldClient users that have MDaemon accounts are imported.

Version 4 Special Notes

In the MDaemon.ini file, the extra local and remote queue key names have been changed. If you are using this feature then you will need to manually edit your MDaemon.ini file and change these keys from:

LocalQueueX to LocalQX (where X is the decimal queue number)

RemoteQueueX to RemoteQX (where X is the decimal queue number)

RAWQueueX to RAWQX (where X is the decimal queue number)

The API has been greatly expanded (see MD-API.HTML). Due to this expansion, your custom programs may need to be recompiled.

Version 3 Special Notes

MDaemon Version 3 incorporated many changes to its internal structure and many of its supporting DAT configuration files. Because of these changes, the installation process automatically migrates version 2.x configuration files to the new version formats where appropriate. If upgrading from version 2.x, your old v2.x files are backed up and placed in the \OLDFILES\ directory during the installation process.

The addition of full multiple domain support made it necessary to change several supporting DAT file formats, including the USERLIST.DAT file. Consequently, version 3 and later is completely incompatible with the discontinued WebPOP series of products from Alt-N Technologies. WebPOP is no longer supported and will not be updated. Instead, we provide our customers with WorldClient, which improves dramatically on the basic WebPOP idea.

There is no longer a POP logon field within the user database. In keeping with a common industry standard, the Mailbox value is also used as the POP logon. If you have accounts that maintain different values for their Mailbox and POP logon, the conversion process, which is invoked automatically during installation, changes these account records to use the old logon value as the new mailbox. Then, aliases (page 256) are created for the new mailbox value in order to prevent your users from having to reconfigure their mail client or change their email address. Thus, their old Mailbox name is an alias for their new Mailbox. The TRACKPOP.TXT file lists accounts that are updated in this manner. Further, in keeping with the removal of a stand-alone POP logon field, the $POPNAME$ macro was discontinued. The conversion utility scans the appropriate .DAT files and removes this macro.

There is no longer a separate field in the user database for a \FILES\ directory. Now, an account's \FILES\ directory is always within its mail directory in a subdirectory called \FILES\. The conversion utility (automatically invoked during installation) adds entries to a file called TRACKDIR.TXT, which details any incompatibilities this might cause for any of your accounts. Additionally, there is no longer a separate \FILES\ directory for Domain Gateways. The \FILES\ subdirectory is always maintained as part of the overall mail directory.

The aliasing system (page 256) was completely redesigned. Aliased accounts will be modified, therefore go to the 'Address Aliases' selection from the 'Setup' menu and carefully inspect your aliases as soon as possible.

Installation

MDaemon Server v6 requires a Microsoft Windows 95 OSR2, NT4, 2000, or better computer system with a Pentium III 500MHz equivalent microprocessor and 256 MB of RAM or better (a 1 GHz computer with 1 GB of RAM is recommended). SMTP/POP/IMAP and related services require a Winsock compliant TCP/IP stack, such as that which ships with Microsoft Windows, and Internet access with an ISP service. If you will be using MDaemon as an internal email server only (you will not be using it to send or receive messages externally) then an Internet Service Provider is not necessary.

To install **MDaemon Server v6** click **Start→Run…** and enter the path to the setup executable file provided in your **MDaemon** package, then click **OK**. Alternatively, you may install MDaemon by using "Add/Remove Programs" located in the Control Panel.

The installation process will prompt you for some basic information such as a registration name and a root directory where **MDaemon** files should be created. The installation process also provides a step-by-step configuration wizard that can be used to guide you through the most common configuration scenarios.

See:

Primary Domain Configuration—page 34
New Account Defaults—page 216

See also:

DomainPOP Mail Collection—page 152

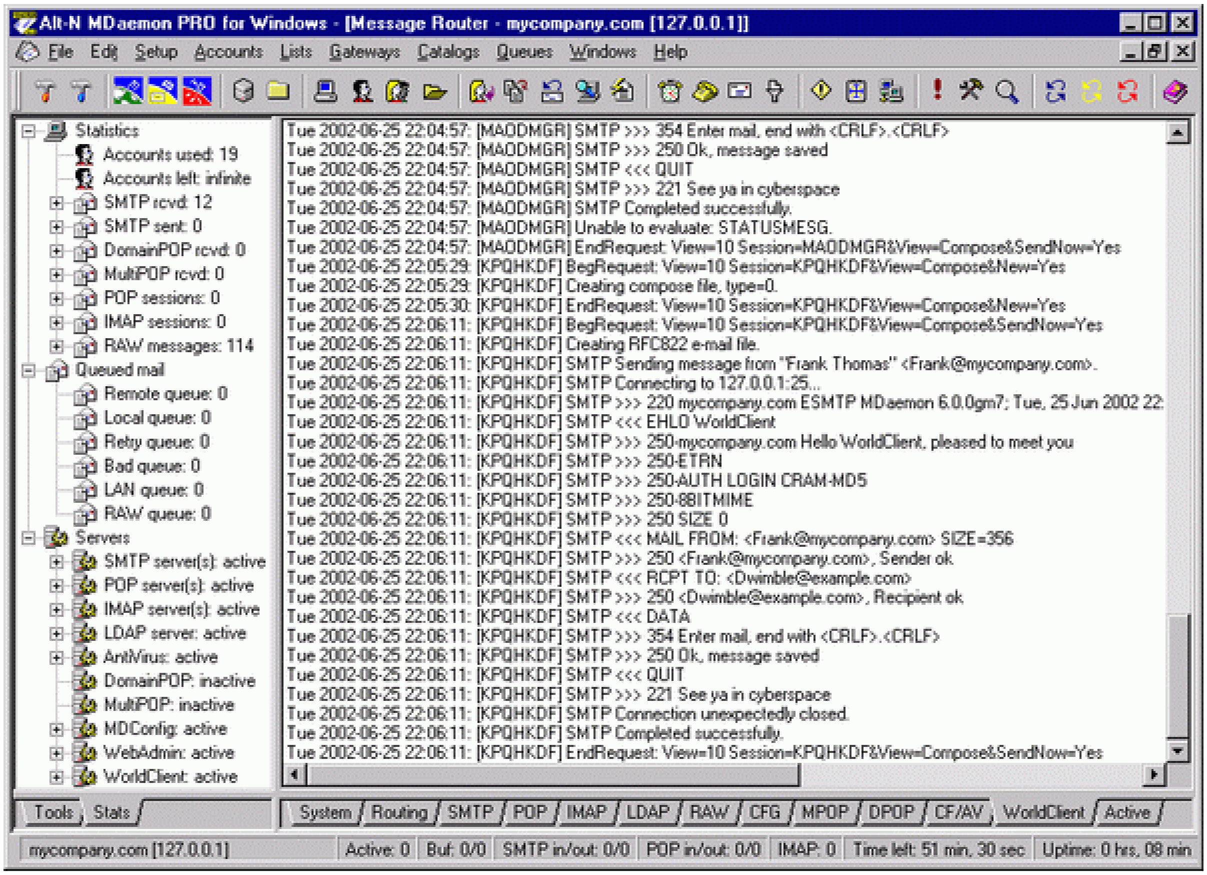
Chapter

2

MDaemon's Main Display

Message Router

MDaemon's Message Router automatically appears at program startup and gives you important information regarding MDaemon's resources, statistics, active sessions, and queued mail waiting to be processed. It also contains controls for easily activating/deactivating MDaemon's various servers. The Message Router's tabbed frames keep you up to date on how the server and its incoming and outgoing connections are performing.


Alt-N MDaemon PRO for Windows - [Message Router - mycompany.com [127.0.0.1]]
File Edit Setup Accounts Lists Gateways Catalogs Queues Windows Help
Tools
Stats
System
Routing
SMTP
POP
IMAP
LDAP
RAW
CFG
MPOP
DPOP
CF/AV
WorldClient
Active

```
Statistics
    Accounts used: 19
    Accounts left: infinite
    SMTP rcvd: 12
    SMTP sent: 0
    DomainPOP rcvd: 0
    MultiPOP rcvd: 0
    POP sessions: 0
    IMAP sessions: 0
    RAW messages: 114
Queued mail
    Remote queue: 0
    Local queue: 0
    Retry queue: 0
    Bad queue: 0
    LAN queue: 0
    RAW queue: 0
Servers
    SMTP server(s): active
    POP server(s): active
    IMAP server(s): active
    LDAP server: active
    AntiVirus: active
    DomainPOP: inactive
    MultiPOP: inactive
    MDConfig: active
    WebAdmin: active
    WorldClient: active
```

```
Tue 2002-06-25 22:04:57: [MAODMGR] SMTP >>> 354 Enter mail, end with <CRLF>.<CRLF>
Tue 2002-06-25 22:04:57: [MAODMGR] SMTP >>> 250 Ok, message saved
Tue 2002-06-25 22:04:57: [MAODMGR] SMTP <<< QUIT
Tue 2002-06-25 22:04:57: [MAODMGR] SMTP >>> 221 See ya in cyberspace
Tue 2002-06-25 22:04:57: [MAODMGR] SMTP Completed successfully.
Tue 2002-06-25 22:04:57: [MAODMGR] Unable to evaluate: STATUSMESG.
Tue 2002-06-25 22:04:57: [MAODMGR] EndRequest: View=10 Session=MAODMGR&View=Compose&SendNow=Yes
Tue 2002-06-25 22:05:29: [KPQHKDF] BegRequest: View=10 Session=KPQHKDF&View=Compose&New=Yes
Tue 2002-06-25 22:05:29: [KPQHKDF] Creating compose file, type=0.
Tue 2002-06-25 22:05:30: [KPQHKDF] EndRequest: View=10 Session=KPQHKDF&View=Compose&New=Yes
Tue 2002-06-25 22:06:11: [KPQHKDF] BegRequest: View=10 Session=KPQHKDF&View=Compose&SendNow=Yes
Tue 2002-06-25 22:06:11: [KPQHKDF] Creating RFC822 e-mail file.
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP Sending message from "Frank Thomas" <Frank@mycompany.com>.
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP Connecting to 127.0.0.1:25...
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 220 mycompany.com ESMTP MDaemon 6.0.0gm7; Tue, 25 Jun 2002 22:
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP <<< EHLO WorldClient
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250-mycompany.com Hello WorldClient, pleased to meet you
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250-ETRN
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250-AUTH LOGIN CRAM-MD5
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250-8BITMIME
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250 SIZE 0
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP <<< MAIL FROM: <Frank@mycompany.com> SIZE=356
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250 <Frank@mycompany.com>, Sender ok
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP <<< RCPT TO: <Dwimble@example.com>
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250 <Dwimble@example.com>, Recipient ok
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP <<< DATA
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 354 Enter mail, end with <CRLF>.<CRLF>
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 250 Ok, message saved
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP <<< QUIT
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP >>> 221 See ya in cyberspace
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP Connection unexpectedly closed.
Tue 2002-06-25 22:06:11: [KPQHKDF] SMTP Completed successfully.
Tue 2002-06-25 22:06:11: [KPQHKDF] EndRequest: View=10 Session=KPQHKDF&View=Compose&SendNow=Yes
```

```
mycompany.com [127.0.0.1] | Active: 0 | Buf: 0/0 | SMTP in/out: 0/0 | POP in/out: 0/0 | IMAP: 0 | Time left: 51 min, 30 sec | Uptime: 0 hrs, 08 min
```

Statistics and Tools

The default left pane of MDaemon's main interface contains two tabs: Tools and Stats. The Tools tab contains an entry for the Primary Domain and each Secondary Domain. Under each entry there is a shortcut to the various dialogs that can be used to configure that domain's settings and users. The Stats tab contains three sections: Statistics, Queued Mail, and Servers. Right-click any of the controls in a section to open a shortcut menu relevant to that control.

The *Statistics* section contains statistics regarding the number of messages sent and received by MDaemon as well as the number of mail sessions that have been initiated since startup. This section also tells you how many user accounts have been used and how many more can be created. *Statistics* contains two right-click shortcut menus: one for the Accounts controls and one for the Statistics controls. The Accounts shortcut menu provides shortcuts for creating, editing, and deleting accounts. The rest of the controls have a shortcut menu that can be used to clear the count listed next to the given control.

The *Queued Mail* section contains an entry for each message queue, and the number of messages (if any) that each queue contains. Each control's shortcut menu can be used to process the queue and open the Queue and Statistics Manager, which can be used for viewing, copying, or deleting the contents of the queue, as well as a number of other functions.

The *Servers* section contains an entry for each server within MDaemon, and each entry lists the current state of the server: "Active" or "Inactive". Listed below each entry is the port on which that particular server is listening, if that server is currently active. The shortcut menu provides a control for toggling each server between the Active and Inactive state.

Message and Event Tracking

The default right-hand pane of the main interface contains several tabs. They display the status of MDaemon's various servers and resources and are frequently updated to reflect current server conditions. Each SMTP/POP/IMAP session and other server activity is logged onto the appropriate tab once it is complete so that a visible record of network activity is made available. The information displayed on these tabs is mirrored in the log files kept in the *Logs* directory, if you have chosen to log such activity. See page 188 for more information.

The Message Router contains the following tabs:

System – At program startup, the System tab displays a log of the *Initialization Process*, which can alert you to possible problems with MDaemon's configuration or status. It also displays activity such as enabling/disabling any of MDaemon's various servers.

Routing – Displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

SMTP – All send/receive session activity using the SMTP protocol is displayed on this tab.

POP – When users collect email from MDaemon using the POP3 protocol, that activity is logged here.

IMAP – Mail sessions using the IMAP protocol are logged on this tab.

RAW – RAW or system generated message activity is logged on this tab.

CFG – All MDConfig activity is displayed on the CFG tab.

MPOP – This tab displays MDaemon's MultiPOP mail collection activities.

DPOP – This tab displays MDaemon's DomainPOP activity.

CF/AV – MDaemon's Content Filter and AntiVirus operations are listed on this tab. When a message is scanned for viruses or matches the criteria of one of the Content Filter's message rules, the relevant information related to that message and the actions taken are logged here.

WorldClient – Displays WorldClient's session activities.

Active – This tab displays an entry for each active connection to MDaemon. Whether SMTP, POP, IMAP, WorldClient, or other type of connection, information about that connection is displayed here.

Note

The information displayed on these tabs has no affect on the amount of data that is actually stored in the log files. However, MDaemon does support a great deal of flexibility with regard to the amount and type of information that is logged in those files. See the Log File dialog (page 188) for more information on logging options.

Composite Log View

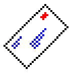
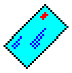
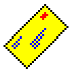
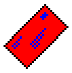
Located on the Windows menu of MDaemon's menu bar is a Composite log view option. Clicking that option will add a window to the router that will combine the information displayed on one or more of the router's tabs. Use the controls on the Miscellaneous Options dialog's GUI tab (page 194) to designate which tabs' information to combine in that window.

Note

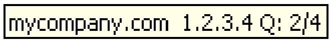
The layout of the panes in the Message Router window is not limited to the default positions described above. You may change the layout be selecting the **Windows** menu selection and then clicking the **Switch panes** control corresponding to the desired layout.

Tray Icon

Whenever the MDaemon server is running, its icon will be visible in the system tray. However, apart from simply letting you know whether the server is running, the icon is also dynamic and will change colors based upon the current server status. The following is a list of the icon indicators:

	All okay. No mail in local or remote queues.
	All okay. Mail in local or remote queues.
	Available disk space below threshold (see page 205).
	Network is down, dialup failed, or disk is full.
Icon Blinking	A newer version of MDaemon is available.

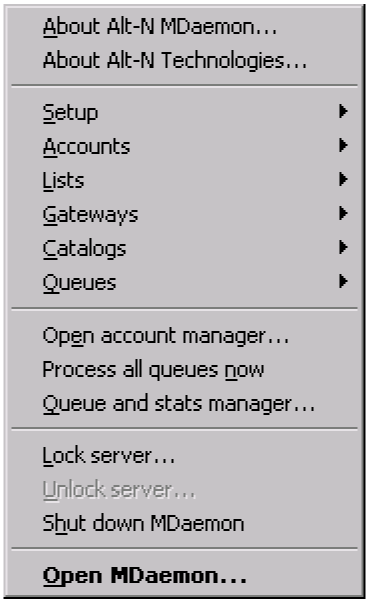
There is additional information about the server available through the icon's tooltip. Pause the mouse pointer over it and the tool tip will appear.



mycompany.com 1.2.3.4 Q: 2/4

The first bit of information that the tool tip displays is the Primary Domain's name. Next is its IP address. Finally, following the letter "Q" (signifying the mail queues), are two numbers denoting the number of messages in the queues. The first numbers indicates the number of messages in the remote queue. The second number indicates the number of messages in the local queue.

Shortcut Menu



Right click on MDaemon's tray icon to open the shortcut menu. This menu gives you quick access to virtually all of MDaemon's menus and features without having to open the main user interface.

Click the "About Alt-N…" options in the top section of the shortcut menu to find out more about MDaemon or Alt-N Technologies.

In the second section you can access the following MDaemon menus: Setup, Accounts, Lists, Gateways, Catalogs, and Queues. Each of these cascading menus is identical to the menu of the same name located on the menu bar of the main interface.

The third section has controls to open the Account Manager and Queue and Statistics manager, and one that will cause all of MDaemon's mail queues to be processed.

Next, there are controls to lock and unlock MDaemon's interface and to shut down MDaemon altogether.

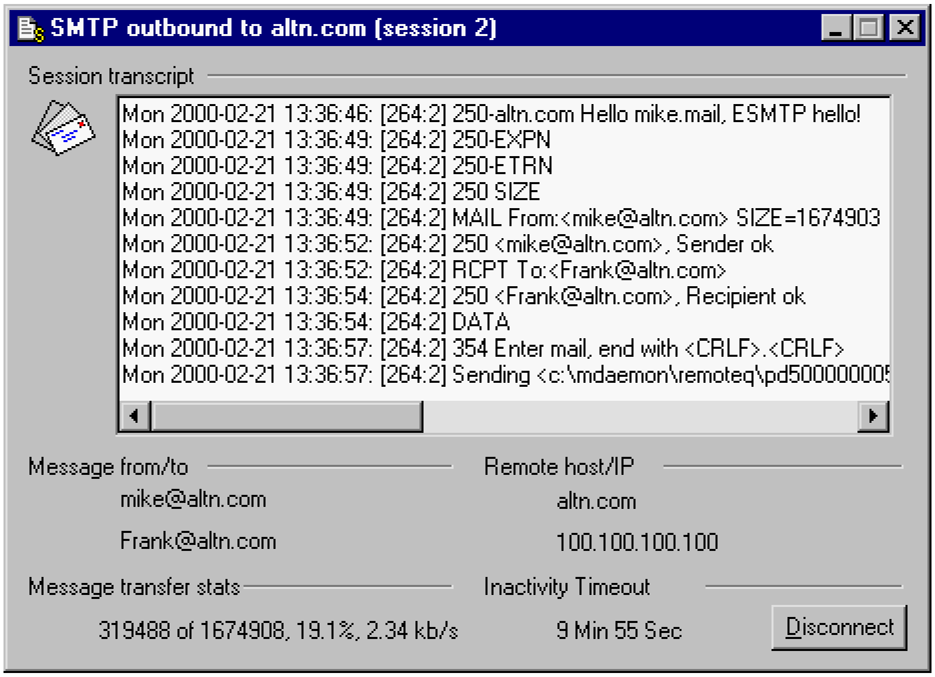
Locking/Unlocking MDaemon's Main Interface

To lock the user interface, minimize MDaemon, click the "Lock server…" control and then enter a password into the dialog that opens. After confirming the password by entering it a second time, MDaemon's user interface will be locked; it cannot be opened or viewed, though MDaemon will continue to function normally. However, you will still be able to use the "Process all queues now…" control on this menu to process the mail queues manually if you desire. To unlock MDaemon, double-click the tray icon or right-click the icon and choose "Open MDaemon…" or "Unlock Server…" and then enter the password that you created when you locked it.

Last, you can open the MDaemon server's interface by clicking the "**Open MDaemon…**" menu selection.

Connection Window

A Connection Window appears each time a request is detected by the server from some remote client, or whenever a session is initiated by the server to collect or deliver a message. This window keeps you informed of the status of the transaction and alerts you to any problems encountered during the course of the mail session.



SMTP outbound to altn.com (session 2)

Session transcript

```
Mon 2000-02-21 13:36:46: [264:2] 250-altn.com Hello mike.mail, ESMTP hello!
Mon 2000-02-21 13:36:49: [264:2] 250-EXPN
Mon 2000-02-21 13:36:49: [264:2] 250-ETRN
Mon 2000-02-21 13:36:49: [264:2] 250 SIZE
Mon 2000-02-21 13:36:49: [264:2] MAIL From:<mike@altn.com> SIZE=1674903
Mon 2000-02-21 13:36:52: [264:2] 250 <mike@altn.com>, Sender ok
Mon 2000-02-21 13:36:52: [264:2] RCPT To:<Frank@altn.com>
Mon 2000-02-21 13:36:54: [264:2] 250 <Frank@altn.com>, Recipient ok
Mon 2000-02-21 13:36:54: [264:2] DATA
Mon 2000-02-21 13:36:57: [264:2] 354 Enter mail, end with <CRLF>.<CRLF>
Mon 2000-02-21 13:36:57: [264:2] Sending <c:\mdaemon\remoteq\pd50000000
```

Message from/to
mike@altn.com
Frank@altn.com

Remote host/IP
altn.com
100.100.100.100

Message transfer stats
319488 of 1674908, 19.1%, 2.34 kb/s

Inactivity Timeout
9 Min 55 Sec

<u>Session transcript</u>
This window displays all session i/o.

<u>Remote host/IP</u>
This window tells you the name and IP address of the remote computer MDaemon with which MDaemon is interacting.

<u>Message from/to</u>
This window displays the sender's address and the address of the intended recipients.

<u>Message transfer statistics</u>
This keeps a running total of the number of bytes transmitted to or collected from the remote system, the percentage completed, and the current speed of the transfer.

<u>Inactivity timeout</u>
This counter displays how much inactivity time is left before MDaemon will close the session.

<u>Disconnect</u>
This button will immediately disconnect the server from the remote system.

Chapter

3

Primary Domain Configuration

Domain Configuration Editor

The domain configuration editor can be reached via the **SETUP | PRIMARY DOMAIN** menu selection and allows you to enter several key pieces of information regarding your domain setup. Your primary domain is the default domain name and set of configuration options that your users will use to send and receive their email. Only one primary domain can be configured, but MDaemon can manage mail for any number of Secondary Domains, and store mail for any number of *Domain Gateways* as well.

See:

Secondary Domain Editor—page 63
Domain Gateways—page 289

The Domain Configuration editor is a tabbed dialog containing the following sections, which are necessary for configuring MDaemon v6.

Domain/ISP

This dialog contains your Primary Domain's name and IP address. In addition, here you will specify the degree to which you want MDaemon itself to handle delivery of mail versus relaying mail to an ISP or gateway host for them to deliver for you.

Ports

On this dialog, the ports that MDaemon will monitor and use for SMTP and POP email delivery are designated. You will also designate the port on which MDaemon will listen for IMAP events, and the UDP port used for querying DNS servers. In most cases the default settings will not need to be changed. However, being able to configure these port settings is useful when attempting to integrate MDaemon with various other products that you may be using on your system.

DNS

This dialog is used for designating a primary and backup DNS server's IP address. It also contains various controls governing MDaemon's handling of MX and A records and SMTP errors that are encountered during mail delivery.

Timers

This area contains various time limits that MDaemon will observe while connecting to remote hosts, waiting for protocol dialogs, waiting for DNS server responses, and so on. In addition, this dialog contains the *Maximum Message Hop Count* limit, which is used to help prevent messages from being caught in a delivery loop.

Sessions

Here you will designate the maximum number of concurrent session threads that MDaemon will use for sending and receiving SMTP, POP, and IMAP mail. You will also designate the number of messages that MDaemon will attempt to send/receive *at the same time*. In addition, if you so choose, you can set a limit on the number of outbound SMTP messages that will be spooled per session thread.

Dequeue

Use the Dequeue tab to have MDaemon automatically send ETRN, QSND, or similar commands to an ISP in order to have them dequeue email that you may have them "holding" for you so that you can receive this sort of email via SMTP rather than DomainPOP.

Archival

Use the Archival tab to save a copy of all inbound and outbound mail that MDaemon processes. You can also choose whether this archive will include Mailing List or MultiPOP messages or omit them.

Pruning

This tab is used for denoting the amount of time that an account may remain inactive before it will be deleted. It also contains controls for limiting how long messages may be stored.

Pre-Processing

This dialog is used to designate the path to any program that you may want MDaemon to run immediately before processing and delivering of mail. Here you can also set parameters for MDaemon's actions related to this process.

Directories

Here you can specify paths to the locations of various directories that MDaemon will use for Remote and Local queues, work files, archiving, Mailing List Digest files, and so on.

POP Check

As a security measure, many ISPs have begun to require their customers to log in to their POP mailbox before allowing them to send or receive mail through the ISP's mail server. Use this tab to configure MDaemon to do so if necessary.

Unknown Local Mail

This dialog contains various settings that you can use to control what MDaemon will do with messages that arrive at the server addressed to a *Local* domain but to an unknown or undefined user's mailbox. The various control choices include: sending the email message back to the sender, sending it to the Postmaster, putting it in the Bad Message queue, and forwarding the message to another host. These controls may be set to act individually or in any combination.

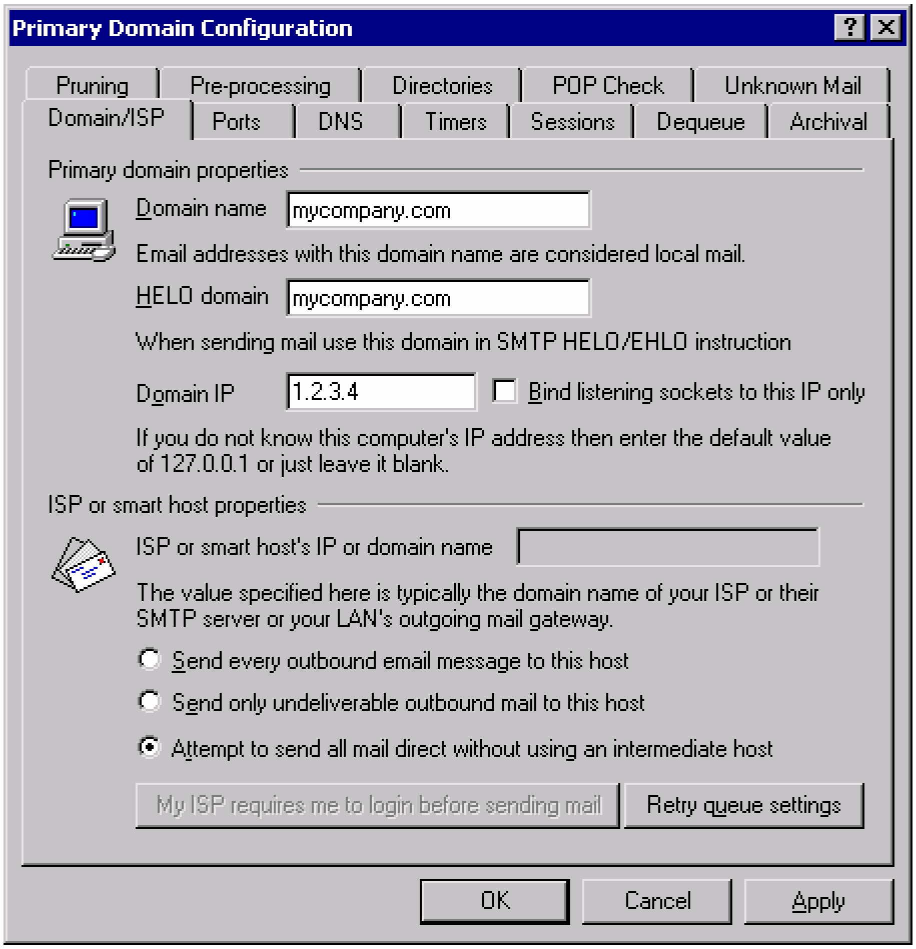
See:

Hosting Multiple Domains—page 62
Domain Gateways—page 289

See Also:

DomainPOP Mail Collection—page 152

Domain/ISP



Primary domain properties

Domain name: mycompany.com

Email addresses with this domain name are considered local mail.

HELO domain: mycompany.com

When sending mail use this domain in SMTP HELO/EHLO instruction

Domain IP: 1.2.3.4 □ Bind listening sockets to this IP only

If you do not know this computer's IP address then enter the default value of 127.0.0.1 or just leave it blank.

ISP or smart host properties

ISP or smart host's IP or domain name:

The value specified here is typically the domain name of your ISP or their SMTP server or your LAN's outgoing mail gateway.

○ Send every outbound email message to this host

○ Send only undeliverable outbound mail to this host

● Attempt to send all mail direct without using an intermediate host

Primary Domain Properties

Domain name

Enter your primary domain name here. This is the default domain name used when creating new accounts. Typically, the value entered here will be the registered Internet domain name that a DNS server resolves to the IP address of the local machine running the server, or a qualified alias of that name.

Alternatively, you may choose to use a fictitious domain name for your Primary Domain Name (such as "company.mail") in some situations. When configuring your server in this way it may be necessary to use the **Header Translation** feature (page 133), and/or the **Domain Name Replacement Engine** (page 157), to enable proper mail distribution.

HELO domain

This Domain name will be used in the SMTP HELO/EHLO instruction when sending mail. In most cases, this will be your Primary Domain Name.

Domain IP

This is the Primary Domain's IP address.

Bind listening sockets to this IP only

Selecting this switch causes MDaemon to bind its listening network sockets using the specific IP address found in the *Domain IP* text box. Ordinarily, this control will only need to be used in certain circumstances when hosting multiple domains.

For more information on this type of configuration, see:

Hosting Multiple Domains—page 62

ISP or Smart Host Properties

ISP or smart host's IP or domain name

Specify your ISP or mail host's name or IP address here. This is generally the SMTP server on your ISP.

Note

Do not enter MDaemon's Primary Domain Name or IP address into this text box. This entry should be an ISP or other mail server that can relay mail for you.

Send every outbound email message to this host

Select this option if you want all outbound email, regardless of its destination domain, to be spooled to a gateway host for routed delivery. If selected, all outbound email will be sent to the host specified in the *ISP or smart host's IP or domain name* field. Typically, this feature is useful during high volume periods when direct message delivery would result in an excessive taxation of server resources.

Send only undeliverable outbound mail to this host

Click this option if you want to spool only undeliverable outbound email to the gateway host specified in the *ISP or smart host's IP or domain name* field. Undeliverable mail is email destined for hosts that could not be resolved to an actual IP address (such as an unregistered gateway to a remote network) or email destined for a host that was resolved properly but could not be connected to directly or is refusing direct connections. Rather than return such mail to its originator, this option causes MDaemon to pass the message off to a more powerful MTA. Sometimes the mail system run by your ISP may have routed methods of mail delivery to which your local server may not have direct access.

Attempt to send all mail direct without using an intermediate host

When this option is chosen, MDaemon will attempt to deliver all mail itself instead of passing it to another host. MDaemon will place undeliverable messages into its Retry System and continue to attempt to deliver them according to the parameters and time intervals that you set in the Retry Configuration dialog. You can access this dialog by clicking the *Retry Queue Settings* button.

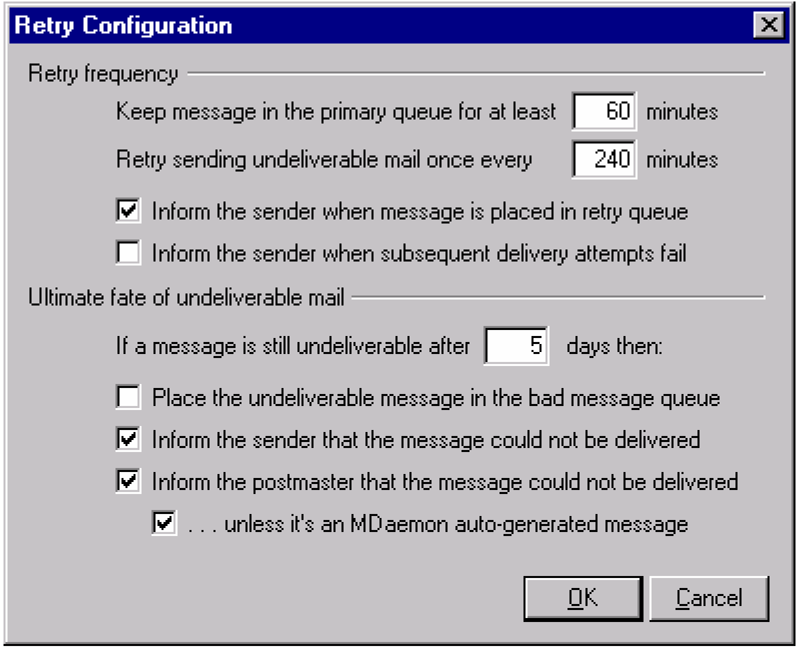
My ISP requires me to log in before sending mail

As a security measure, in order to prevent unauthorized users from attempting to relay mail through their servers, some ISPs require their customers to authenticate themselves via ESMTP AUTH or by first performing a POP check of their email account. If this is the case for your ISP, you can open the ISP AUTH dialog by clicking this button. There you can enter the required authentication information. See ISP AUTH below.

Retry queue settings

Click this button to open the **Retry Configuration dialog** from which you can designate how often MDaemon will attempt to deliver messages which it has thus far been unable to deliver. You can also specify a time interval after which the attempts will cease, and what to do with these messages after the final attempt is made.

Retry Queue Settings



Retry frequency

Keep message in the primary queue for at least 60 minutes

Retry sending undeliverable mail once every 240 minutes

☑ Inform the sender when message is placed in retry queue

☐ Inform the sender when subsequent delivery attempts fail

Ultimate fate of undeliverable mail

If a message is still undeliverable after 5 days then:

☐ Place the undeliverable message in the bad message queue

☑ Inform the sender that the message could not be delivered

☑ Inform the postmaster that the message could not be delivered

☑ . . . unless it's an MDaemon auto-generated message

Retry Frequency

Keep message in the primary queue for at least XX minutes

This setting governs the length of time a message will remain in the primary queue before being removed and placed in the retry queue. The primary queue will generally attempt to deliver the message quicker and more frequently than the retry queue.

Retry sending undeliverable mail once every XX minutes

This setting determines how frequently the messages in the retry queue are processed.

Inform the sender when message is placed in retry queue

This switch will inform the sender when his/her message is removed and placed in the retry queue. The text of this message can be found (and edited) in the `DELWARN.DAT` file.

Inform the sender when subsequent delivery attempts fail

If a delivery attempt of a message in the retry queue fails, a message explaining this fact will be dispatched to the sender of the message. The text of this message can be found (and edited) in the `DELWARN.DAT` file.

Ultimate Fate of Undeliverable Mail

If a message is still undeliverable after XX days then:
This setting determines the number of days that a message can remain in the retry queue before being removed.

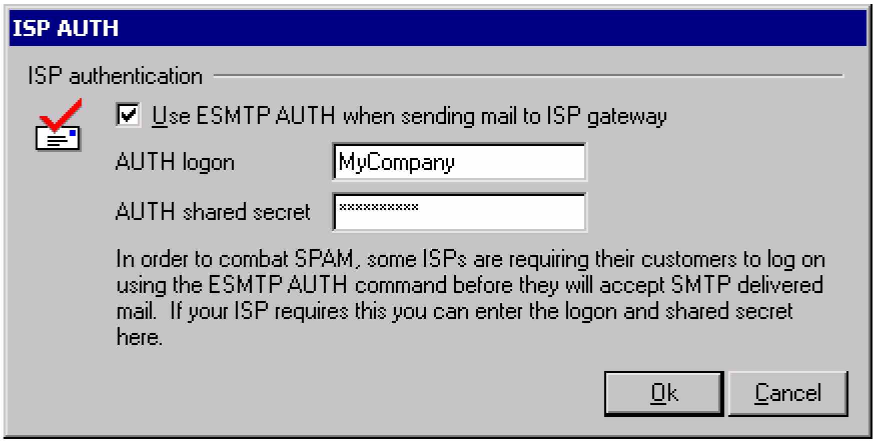
Place the undeliverable message in the bad message queue
Once a message has reached the time limit set in the *If A Message Is Still Undeliverable After xx Days Then:* control, a copy of that message will be moved to the bad message directory if this switch is enabled.

Inform the sender that the message could not be delivered
Once a message has reached the time limit set in the *If A Message Is Still Undeliverable After xx Days Then:* control, this switch will cause MDaemon to send a message to the sender informing them that the message has been permanently removed from the server. The text of this message can be found (and edited) in the `DELERR.DAT` file.

Inform the postmaster that the message could not be delivered
If this switch is enabled, the postmaster will be notified when a message has been permanently removed from the retry system.

. . . unless it's an MDaemon auto-generated message
The retry system will never inform MDaemon when an auto-generated message fails to be delivered. However, because such information may be useful to the postmaster, he or she will be informed when these messages cannot be delivered. Click this checkbox if you do not want the postmaster to be informed when auto-generated messages cannot be delivered. Examples of auto-generated messages are return-receipt notifications, auto-responder generated messages, results of account processing, and so on.

ISP AUTH



☑ Use ESMTP AUTH when sending mail to ISP gateway

AUTH logon: MyCompany

AUTH shared secret: ***********

In order to combat SPAM, some ISPs are requiring their customers to log on using the ESMTP AUTH command before they will accept SMTP delivered mail. If your ISP requires this you can enter the logon and shared secret here.

ISP Authentication

Use ESMTP AUTH when sending mail to ISP gateway
As an added security measure, some ISPs require their customers to log on using the ESMTP AUTH command before they are allowed to send mail through the ISPs servers. If your ISP requires you to do

this then you can use the controls under this section to configure MDaemon to do so. Click this checkbox to cause MDaemon to send your authentication information before it attempts to deliver messages.

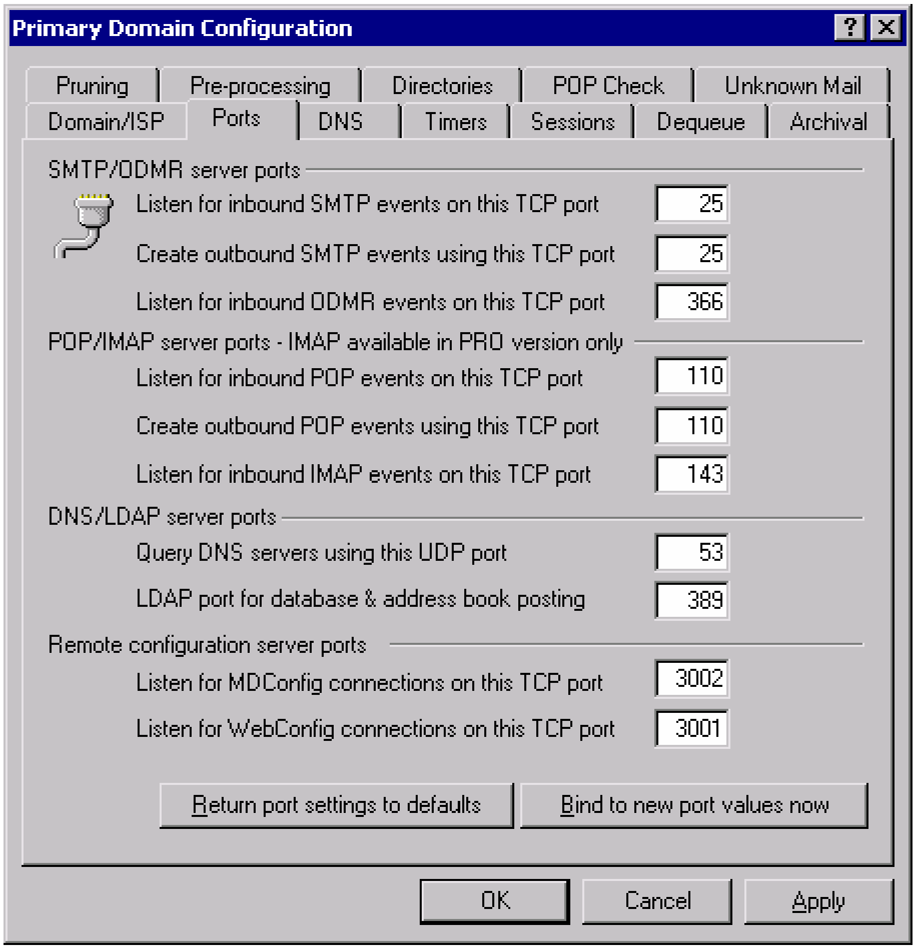
AUTH logon

Enter you AUTH logon here.

AUTH shared secret

This is the password used in the ESMTP AUTH command's shared secret.

Ports



SMTP/ODMR server ports

Listen for inbound SMTP events on this TCP port: 25

Create outbound SMTP events using this TCP port: 25

Listen for inbound ODMR events on this TCP port: 366

POP/IMAP server ports - IMAP available in PRO version only

Listen for inbound POP events on this TCP port: 110

Create outbound POP events using this TCP port: 110

Listen for inbound IMAP events on this TCP port: 143

DNS/LDAP server ports

Query DNS servers using this UDP port: 53

LDAP port for database & address book posting: 389

Remote configuration server ports

Listen for MDConfig connections on this TCP port: 3002

Listen for WebConfig connections on this TCP port: 3001

SMTP/ODMR Server Ports

Listen for inbound SMTP events on this TCP port
MDaemon will monitor this port for incoming connections from SMTP clients.

Create outbound SMTP events using this TCP port
This port will be used when mail is sent to other SMTP servers.

Listen for inbound ODMR events using this TCP port
MDaemon will monitor this port for incoming On-Demand Mail Relay (ODMR) connections such as ATRN from Domain Gateways.

POP/IMAP Server Ports (IMAP Available in MDaemon Pro only)

Listen for inbound POP events on this TCP port
MDaemon will monitor this port for incoming connections from remote POP clients.

Create outbound POP events using this TCP port

This port will be used when mail is retrieved from POP3 servers.

Listen for inbound IMAP events on this TCP port
MDaemon will monitor this port for incoming IMAP requests.

DNS/LDAP Server Ports

Query DNS servers using this UDP port
Enter the Port you want MDaemon to use for sending and receiving data grams to the DNS server.

LDAP port for database & address book posting
MDaemon will post database and address book information to your LDAP server on this port.

See: LDAP Address Book Support—page 94

Remote Configuration Server Port Settings

Listen for MDConfig connections on this TCP port
This is the port that MDaemon will monitor for MDConfig connections (see page 70).

Listen for WebAdmin connections on this TCP port
This is the port that MDaemon will monitor for WebAdmin connections.

Return port settings to defaults
This button returns all the port settings to their standard values.

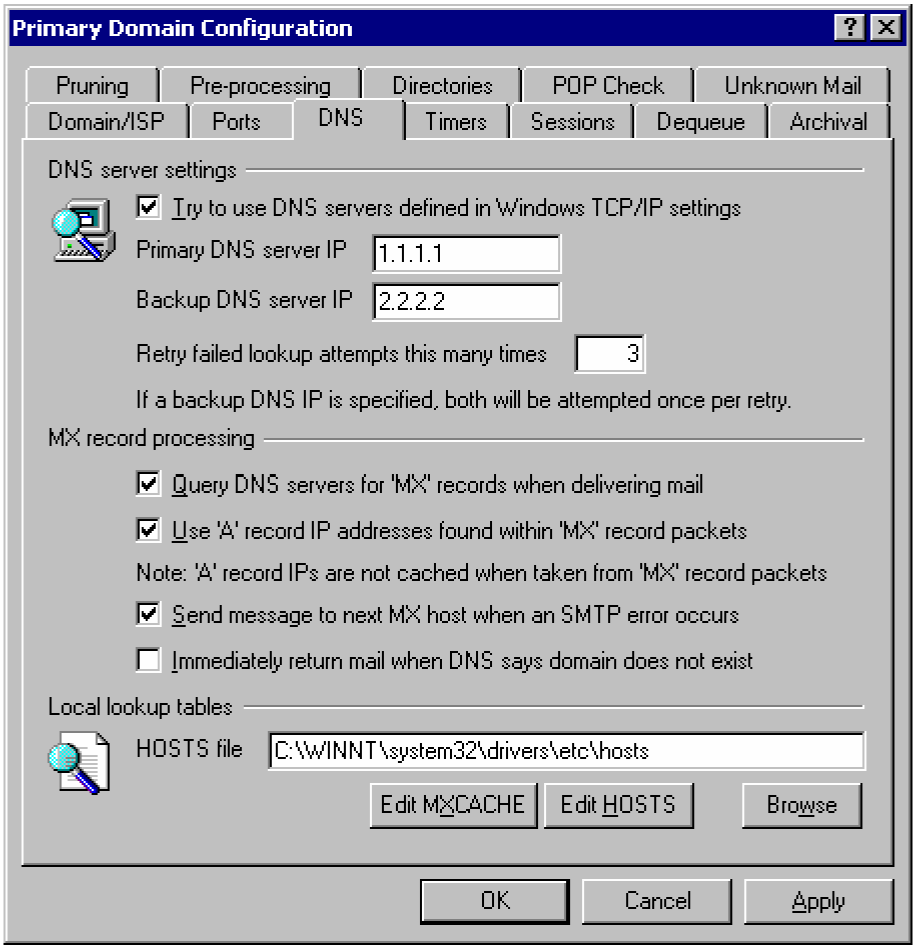
Bind to new port values now
When you alter the values of any of the port settings you will need to press this button to have your changes take immediate effect. Otherwise, your changes will not be put into place until the next time the server is started.

Note

The preceding port settings are critical for proper server operation and should not be altered unless you are certain that you must do so. Being able to configure the ports that MDaemon uses will allow you to configure the server to operate with proxy systems or other software services that require certain port numbers.

An IP address (a machine) has only one of each available port. If another program attempts to gain access to a port that is already in use by another piece of software an **error** message will inform the user that the requested address (IP:PORT) is **already in use**.

DNS



DNS server settings

☑ Try to use DNS servers defined in Windows TCP/IP settings

Primary DNS server IP: 1.1.1.1

Backup DNS server IP: 2.2.2.2

Retry failed lookup attempts this many times: 3

If a backup DNS IP is specified, both will be attempted once per retry.

MX record processing

☑ Query DNS servers for 'MX' records when delivering mail

☑ Use 'A' record IP addresses found within 'MX' record packets

Note: 'A' record IPs are not cached when taken from 'MX' record packets

☑ Send message to next MX host when an SMTP error occurs

□ Immediately return mail when DNS says domain does not exist

Local lookup tables

HOSTS file: C:\WINNT\system32\drivers\etc\hosts

DNS Server Settings

Try to use DNS servers defined in windows TCP/IP settings

Windows sometimes keeps a DNS server IP address in the local TCP/IP configuration. If this is the case on your computer then you can check this option. If MDaemon cannot find a locally maintained DNS server it will continue on and use the ones specified on this screen.

Primary DNS server IP address

Enter the IP address of the DNS server that you want MDaemon to query for 'A' and 'MX' records. In order to ensure proper operation this entry must be specified.

Backup DNS server IP address

Enter the IP address of the backup or secondary DNS server that you want MDaemon to query for 'A' and 'MX' records. This entry is optional but recommended.

Retry failed lookup attempts this many times

If for some reason a lookup attempt fails, this is the number of times that MDaemon will repeat the attempt. If you have designated a backup DNS server, both servers will be included in each lookup attempt.

MX Record Processing

Query DNS servers for 'MX' records when delivering mail
Enable this control if you want MDaemon to query your designated DNS servers for 'MX' records when it is attempting to deliver mail.

Use 'A' record IP addresses found within 'MX' record packets
Click this checkbox if you want MDaemon to attempt delivery to 'A' record IP addresses when such are discovered during 'MX' record processing.

Send message to next MX host when an SMTP error occurs
With this function active, MDaemon will continue to attempt message delivery to the next 'MX' hosts even if the current 'MX' returns a fatal SMTP error.

Immediately return mail when DNS says domain does not exist
This switch will cause MDaemon to immediately return a message if a DNS lookup returns a "Domain Does Not Exist" message. This will prevent this sort of mail from needlessly going into the delivery retry cycle.

Local Lookup Tables

Hosts file…
Before querying the DNS servers, MDaemon will first attempt to resolve an address by processing the Windows HOSTS file. If this file contains the IP address of the domain in question, MDaemon will not need to query the DNS server.

Note

You must enter the complete path and filename rather than just the filename. MDaemon will attempt to use the following values as the default location of this file:

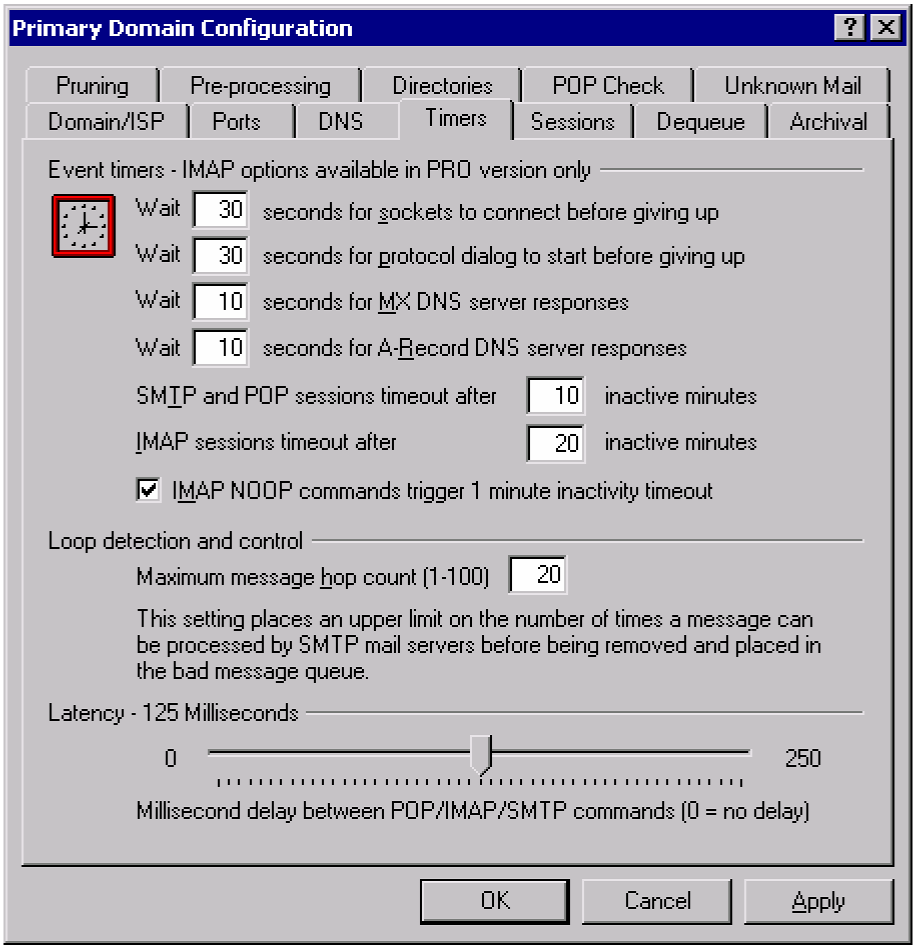
```
Windows 95/98 - [drive]:\windows\hosts
Windows NT - [drive]:\windows\system32\drivers\etc\hosts
```

The HOSTS file is a Windows file that contains the A-record or primary IP address for a domain name. MDaemon also allows you to specify MX-record IP addresses within a file called MXCACHE.DAT. This file can be found within the MDaemon\APP\ subdirectory. Load the MXCACHE.DAT file into a text editor and read the comments at the top of the file for more information.

Edit MXCACHE file
Click this button to view or edit the MXCACHE.DAT file with MDaemon's text editor.

Edit hosts File
Click this button to view or edit the HOSTS file with MDaemon's text editor.

Timers



Event timers - IMAP options available in PRO version only

Wait 30 seconds for sockets to connect before giving up

Wait 30 seconds for protocol dialog to start before giving up

Wait 10 seconds for MX DNS server responses

Wait 10 seconds for A-Record DNS server responses

SMTP and POP sessions timeout after 10 inactive minutes

IMAP sessions timeout after 20 inactive minutes

☑ IMAP NOOP commands trigger 1 minute inactivity timeout

Loop detection and control

Maximum message hop count (1-100) 20

This setting places an upper limit on the number of times a message can be processed by SMTP mail servers before being removed and placed in the bad message queue.

Latency - 125 Milliseconds

0 250

Millisecond delay between POP/IMAP/SMTP commands (0 = no delay)

Event Timers (IMAP options available in Pro version only)

Wait XX seconds for sockets to connect before giving up

After initiating a connection request MDaemon will wait this many seconds for the remote system to accept the connection. If the remote system does not respond within this time frame MDaemon will send the message to either the Gateway Host or Retry Queue depending upon which option you have chosen on the **Domain/ISP** tab (page 36) of the Domain Configuration Editor.

Wait XX seconds for protocol dialog to start before giving up

Once a connection has been established with a remote host, this is the number of seconds that MDaemon will wait for the remote host to begin the SMTP or POP3 protocol dialog. If the remote host does not begin the protocol session within this time frame MDaemon will send the message to either the Gateway Host or Retry Queue depending upon which option you have chosen on the **Domain/ISP** tab (page 36) of the Domain Configuration Editor.

Wait XX seconds for MX DNS server responses

While using DNS services to resolve 'MX' hosts for remote domains, MDaemon will wait for responses to its 'MX' queries for this number of seconds. If the DNS server does not respond within this time frame MDaemon will attempt to deliver the message to the IP address specified in the remote host's 'A' DNS record. If that attempt fails MDaemon will send the message to either the Gateway Host or Retry Queue depending upon which option you have chosen on the **Domain/ISP** tab (page 36) of the Domain Configuration Editor.

Wait XX seconds for A-record DNS server responses

This timer governs how long MDaemon will wait while attempting to resolve a remote host's IP address. If the attempt fails, MDaemon will send the message to either the Gateway Host or Retry Queue depending upon which option you have chosen on the **Domain/ISP** tab (page 36) of the Domain Configuration Editor.

SMTP and POP sessions timeout after XX inactive minutes

If a successfully connected and operating session remains inactive (no i/o) for this length of time, MDaemon will abort the transaction. MDaemon will try again at the next scheduled processing interval.

IMAP sessions timeout after XX inactive minutes

If an IMAP session has no activity for this number of minutes, MDaemon will close the session.

IMAP NOOP commands trigger 1 minute inactivity timeout

When this checkbox is enabled, the IMAP inactivity timer will be set to one minute when a NOOP command is encountered. Some IMAP clients will issue NOOP commands simply to keep sessions open even though there is no actual mail transaction activity going on. This feature will prevent such sessions from remaining active and thus will reduce resources consumed, which can be extremely useful for higher volume IMAP based mail sites.

Loop Detection and Control

Maximum message hop count (1-100)

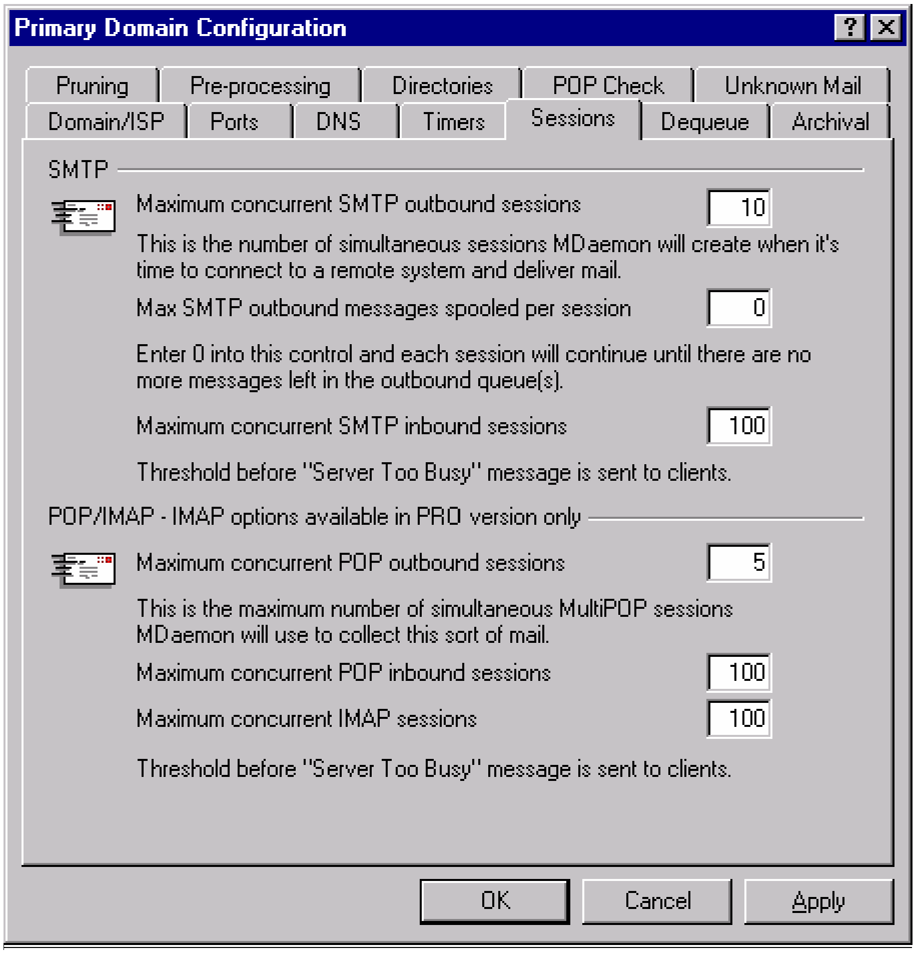
RFC standards stipulate that a mail server must stamp each message each time that it is processed. These stamps can be counted and used as a stopgap measure against recursive mail loops that can sometimes be caused by errant configurations. If undetected, these looping message delivery cycles will consume your resources. By counting the number times the message has been processed, such messages can be detected and placed in the bad message directory. The assumption is that if a message hasn't reached its recipient after being processed by a given number of mail servers then there is probably a mail loop in progress. Most likely, the default setting of this control should be sufficient to prevent mail loops and will not need to be changed.

Latency

Latency – XX milliseconds

This is the delay in milliseconds between POP/SMTP/IMAP protocol commands. This is useful for preventing high-speed connections from processing data faster than the recipient can extract it. This delay takes effect only during the POP/SMTP/IMAP protocol command sequence – the actual transfer of a mail message file is already fully buffered.

Sessions



Maximum concurrent SMTP outbound sessions: 10

This is the number of simultaneous sessions MDaemon will create when it's time to connect to a remote system and deliver mail.

Max SMTP outbound messages spooled per session: 0

Enter 0 into this control and each session will continue until there are no more messages left in the outbound queue(s).

Maximum concurrent SMTP inbound sessions: 100

Threshold before "Server Too Busy" message is sent to clients.

Maximum concurrent POP outbound sessions: 5

This is the maximum number of simultaneous MultiPOP sessions MDaemon will use to collect this sort of mail.

Maximum concurrent POP inbound sessions: 100

Maximum concurrent IMAP sessions: 100

Threshold before "Server Too Busy" message is sent to clients.

SMTP

Maximum concurrent SMTP outbound sessions

The value entered here represents the maximum possible outbound SMTP sessions that will be created when it is time to send outbound mail. Each session will send outbound messages until either the queue is empty or the *Max SMTP outbound messages spooled per session* setting has been reached. For example, if the outbound mail queue has twenty messages waiting when it is time to send mail and the value of this setting is five, then five sessions will be simultaneously created and each will consecutively deliver four messages.

You should experiment with the number of sessions that yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded or your Windows machine will run out of resources and you will lose delivery efficiency. Remember, each SMTP session created by MDaemon will deliver messages consecutively and therefore four sessions delivering two messages each might perform better and faster than eight threads delivering only one message each. A good place to start would be five to ten threads when using a 28.8k modem and ten to fifteen for ISDN.

Maximum SMTP outbound messages spooled per session

This setting places a limit on the number of individual messages that each session will send before it stops delivering mail and frees itself from memory. Ordinarily, you should leave this control set to zero, which will cause each session to continue delivering messages until the queue is empty.

Maximum concurrent SMTP inbound sessions

This value controls the number of concurrent inbound SMTP sessions that the server will accept before it begins responding with a "Server Too Busy" message.

POP/IMAP (IMAP option available in Pro version only)

Maximum concurrent POP outbound sessions

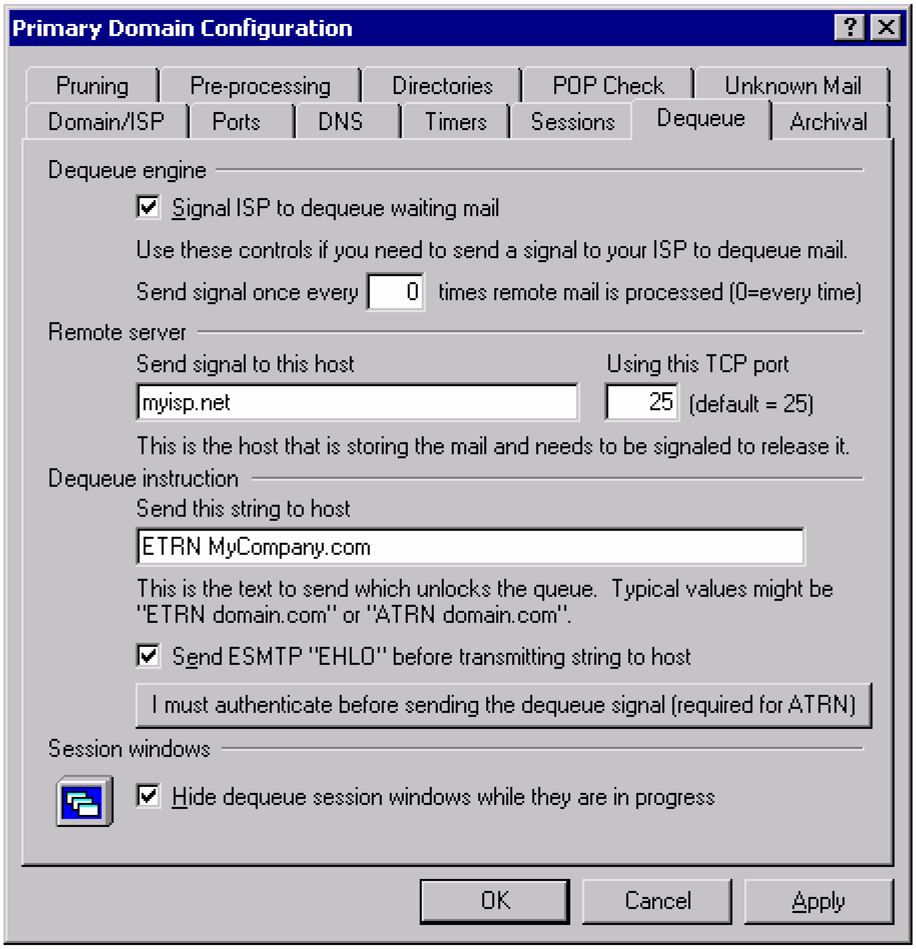
The value entered here represents the maximum possible outbound POP sessions that will be created when it is time to collect DomainPOP and MultiPOP mail. Each session will collect this type of mail until all DomainPOP and MultiPOP servers have been processed, and all mail has been collected. For example, if there are fifteen MultiPOP sessions amongst all of your users and the value of this setting is set to three, then each session will collect mail from five MultiPOP sources.

You should experiment with the number of sessions to determine what number will yield the best performance for your bandwidth. It is possible to specify so many sessions that your bandwidth will be overloaded, or your Windows machine will run out of resources and you will lose processing efficiency. Remember that each POP sessions created by MDaemon will collect mail until all sources have been exhausted. Therefore, four sessions collecting mail from twenty sources might perform better and faster than twenty sessions collecting from a single source. A good place to start would be two to five sessions with a 28.8 modem and five to ten for ISDN.

Maximum concurrent POP/IMAP inbound sessions

This value controls the maximum number of concurrent POP and IMAP inbound mail sessions that the server will accept before it begins responding with a "Server Too Busy" message.

Dequeue



Dequeue engine

☑ Signal ISP to dequeue waiting mail

Use these controls if you need to send a signal to your ISP to dequeue mail.

Send signal once every [0] times remote mail is processed (0=every time)

Remote server

Send signal to this host: myisp.net

Using this TCP port: 25 (default = 25)

This is the host that is storing the mail and needs to be signaled to release it.

Dequeue instruction

Send this string to host: ETRN MyCompany.com

This is the text to send which unlocks the queue. Typical values might be "ETRN domain.com" or "ATRN domain.com".

☑ Send ESMTP "EHLO" before transmitting string to host

I must authenticate before sending the dequeue signal (required for ATRN)

Session windows

☑ Hide dequeue session windows while they are in progress

Dequeue Engine

Signal ISP to dequeue waiting mail

When it is time to process remote mail MDaemon can connect to any server on any port and send any string that you wish to send. This is useful when you need to signal a remote server to release your mail by sending some string to them. For example, ATRN, ETRN, or QSND. You can also use this feature when a FINGER or TELNET session is briefly required in order for your ISP to determine that you are online.

Send signal once every [xx] times remote mail is processed

By default the dequeue signal will be sent each time that remote mail is processed. Entering a number into this control will prevent the dequeue signal from being sent every time. It will be sent every x number of times as designated. For example, setting this value to "3" would cause the signal to be sent every third time that remote mail is processed.

Remote Server

Send signal to this remote host

This is the host to which you wish to connect to signal the release of your mail.

Use this TCP port

Enter the port on which you wish to make the connection. The default is 25 (the SMTP port), which is appropriate for the ETRN or QSND signaling method. Port 366 is typically used for ATRN, and port 79 is used for FINGER.

Dequeue Instruction

Send this string to host
This control is for specifying the text string that needs to be sent in order for your email to be released. For example, the ETRN method requires the text "ETRN" followed by the domain name of the site being queued. Other methods require different text to be sent. Consult your ISP if you need more information on what to send to unlock your mail queue.

> **Note**
>
> When using a dequeue method of mail hosting, we recommend using On-Domain Mail Relay (ODMR) whenever possible. We believe that it is currently the best method available for hosting your email in this manner. ODMR requires the ATRN command to be used in this control.

Send SMTP "EHLO" before transmitting string to host
If you enable this checkbox then you should be connecting to an SMTP server to signal release of your mail. This switch causes an SMTP session to be initiated with the specified host and allows the session to progress just beyond the SMTP "EHLO" stage before sending the unlock string.

I must authenticate before sending the dequeue signal (required for ATRN)
As a security measure, in order to prevent unauthorized users from attempting to dequeue their customers' email, some ISPs require their customers to authenticate themselves via ESMTP AUTH before sending the dequeue signal. If this is the case for your ISP, you can open the Dequeue AUTH dialog by clicking this button. There you can enter the required authentication information. See Dequeue AUTH below.

> **Note**
>
> Authentication is required when using the ATRN command to dequeue your email.

Session Windows

Hide dequeue session windows while they are in progress
Click this checkbox if you want to hide sessions windows while they are in progress.

> **Note**
>
> If the value you enter into the *Send Signal To This Host* control is a domain name and not an IP address, MDaemon will perform an MX record resolution of this site in an attempt to

connect to the site's MX IP address. This assumes you have the MX resolution engine switched on and working (see **DNS** on page 43). If the value entered is an IP address and not a domain name then the connection will be made using that IP address.

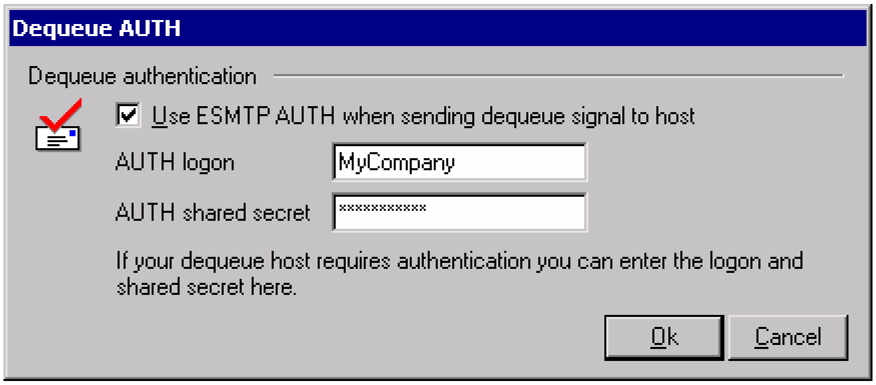
On-Demand Mail Relay (ODMR)

We believe that the best relay (queue/dequeue) method currently available for hosting your email is On-Demand Mail Relay (ODMR). This method is superior to ETRN and other methods in that in requires authentication before mail is dequeued. Further, it utilizes a new ESMTP command called `ATRN` that does not require the client (customer) to have a static IP address because it immediately reverses the flow of data between the client and server (provider) and despools the messages without having to make a new connection to do so (unlike ETRN).

MDaemon fully supports ODMR on the client side via using the `ATRN` command and authentication controls on the Dequeue tab, and on the server side using the Domain Gateways features on the ATRN / AUTH tab of the Gateway Editor (page 294).

Many mail servers do not yet support ODMR, therefore you should check with your provider before attempting to use it.

Dequeue AUTH


Dequeue AUTH

Dequeue authentication

☑ Use ESMTP AUTH when sending dequeue signal to host

AUTH logon: MyCompany

AUTH shared secret: ************

If your dequeue host requires authentication you can enter the logon and shared secret here.

Dequeue Authentication

Use ESMTP AUTH when sending dequeue signal to host

Besides requiring their customers to authenticate themselves before sending mail, some ISPs require their customers to authenticate themselves before sending the signal to dequeue any incoming mail that is being held for them. If you are required to do this then click this checkbox to cause MDaemon to send your authentication information before attempting to collect any queued email.

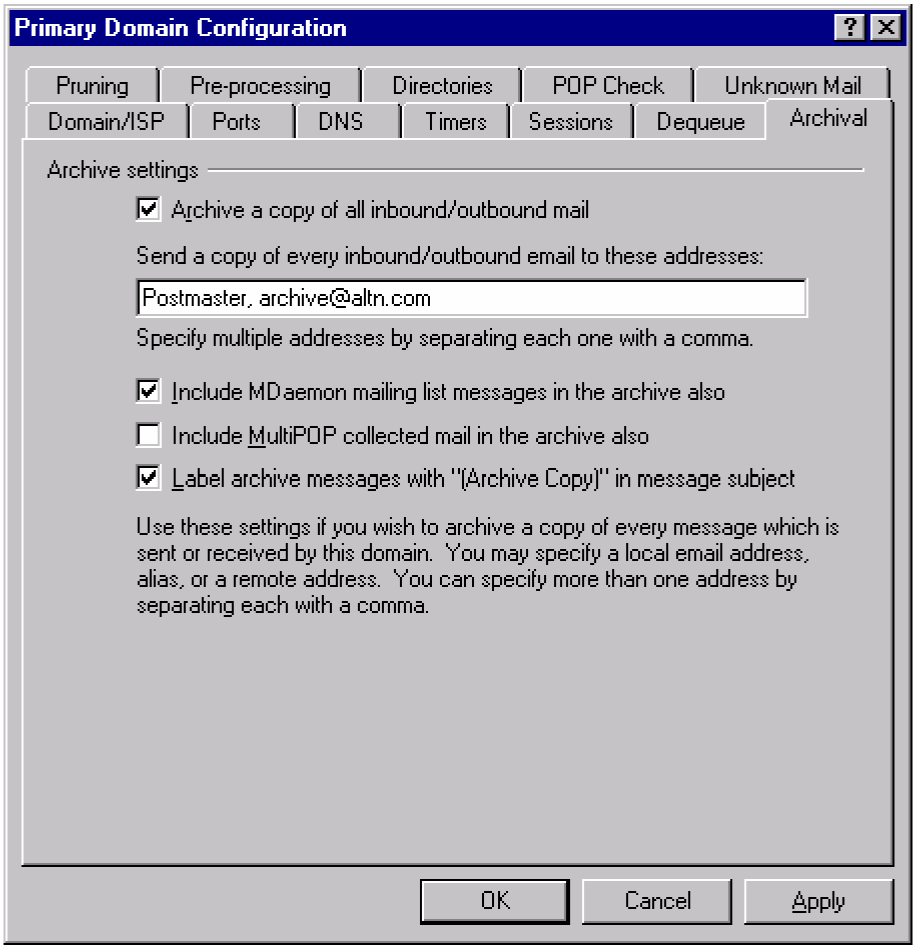
AUTH logon

If authentication is required before sending the signal to dequeue your mail, place the required AUTH logon parameter here.

AUTH shared secret

Enter the password used in the AUTH shared secret required by your ISP.

Archival



Archive settings

☑ Archive a copy of all inbound/outbound mail

Send a copy of every inbound/outbound email to these addresses:

Postmaster, archive@altn.com

Specify multiple addresses by separating each one with a comma.

☑ Include MDaemon mailing list messages in the archive also

☐ Include MultiPOP collected mail in the archive also

☑ Label archive messages with "(Archive Copy)" in message subject

Use these settings if you wish to archive a copy of every message which is sent or received by this domain. You may specify a local email address, alias, or a remote address. You can specify more than one address by separating each with a comma.

Archive Settings

Archive a copy of all inbound/outbound mail

This switch enables the archival engine. Activating it will cause a copy of every inbound and outbound message that passes through the server to be sent to the address(es) specified in the control following.

Send a copy of every inbound/outbound message to these addresses

Enter one or more addresses to which you wish to send archival messages. Multiple addresses must be separated by a comma. You may specify Local and Remote addresses and Address Aliases.

Include MDaemon mailing list messages in the archive also

Select this switch if you want archived mail to include your mailing list messages.

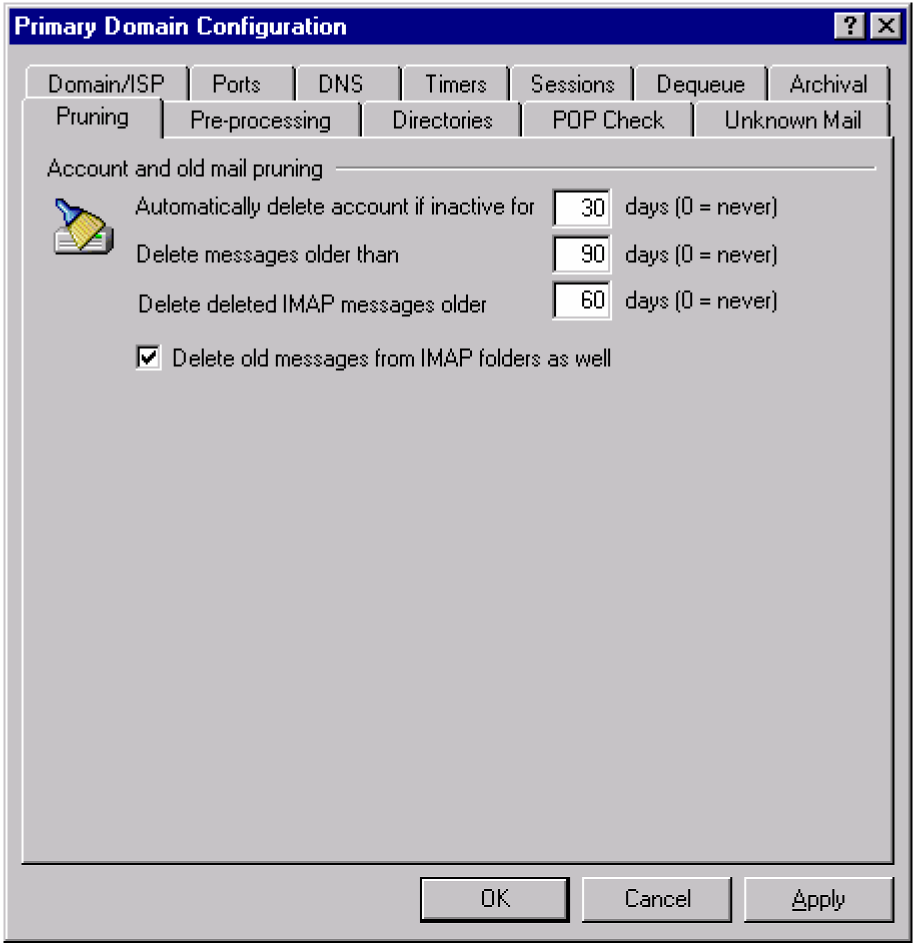
Include MultiPOP collected mail in the archive also

Select this switch if you want archived mail to include messages collected through MDaemon's MultiPOP feature.

Label archive messages with "(archive copy)" in message subject

Enable this switch if you want to include "(Archive Copy)" in the `Subject:` header of archived mail.

Pruning



Account and old mail pruning

Automatically delete account if inactive for 30 days (0 = never)

Delete messages older than 90 days (0 = never)

Delete deleted IMAP messages older 60 days (0 = never)

☑ Delete old messages from IMAP folders as well

The controls on this dialog are used to designate when or if inactive accounts or old messages belonging to this domain will be deleted by MDaemon. Each day at midnight MDaemon will remove all messages and accounts that have exceeded the time limits stated. There are similar controls used for setting these limits for your other domains on the Secondary Domains dialog (page 63). There are also controls on the Account Editor that can be used to override these settings for individual accounts (see page 230).

Note

When old messages are pruned, rather than actually delete them, MDaemon will move them to the "…\BADMSGS\[Mailbox]\" folder where they can be manually deleted later by the administrator or a nightly process. This only applies to pruned old messages – when an account is pruned, it will be deleted along with its messages instead of moved. See `AccountPrune.txt` in the "...MDaemon\App\" folder for more information and command line options.

Account and Old Mail Pruning

Automatically delete account if inactive for XX days (0 = never)

Specify the number of days that you wish to allow an account belonging to this domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

Delete messages older than XX days (0 = never)

A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

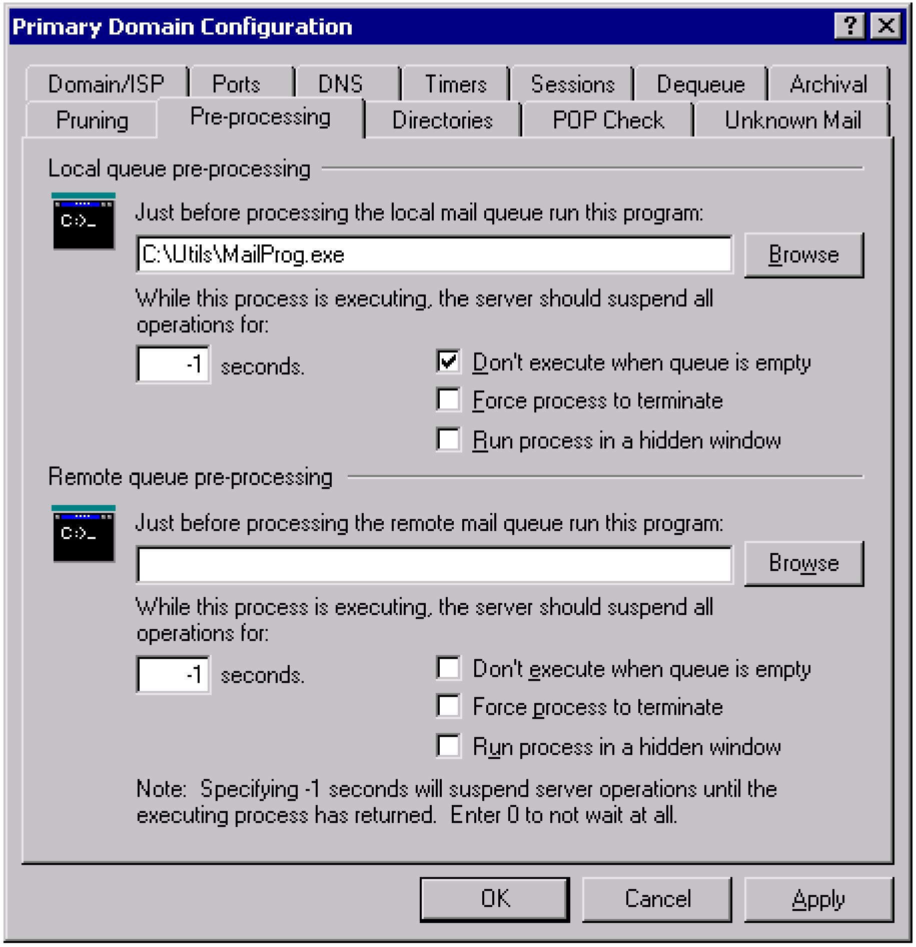
Delete deleted IMAP messages older than XX days (0 = never)

Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in your users' folders. Messages flagged for deletion longer than this number of days will be purged from their mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

Delete old messages from IMAP folders as well

Click this checkbox if you want the "*Delete messages older than…*" control to apply to messages in IMAP folders as well. When this control is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

Pre-processing



Local queue pre-processing

Just before processing the local mail queue run this program: C:\Utils\MailProg.exe

While this process is executing, the server should suspend all operations for: -1 seconds.

☑ Don't execute when queue is empty

□ Force process to terminate

□ Run process in a hidden window

Remote queue pre-processing

Just before processing the remote mail queue run this program:

While this process is executing, the server should suspend all operations for: -1 seconds.

□ Don't execute when queue is empty

□ Force process to terminate

□ Run process in a hidden window

Note: Specifying -1 seconds will suspend server operations until the executing process has returned. Enter 0 to not wait at all.

Local/Remote Queue Pre-processing

Just before processing the (local/remote) mail queue run this program

This field specifies a program path and name that will be executed just prior to the processing and delivery of any RFC-822 messages that might be in the local or remote message queues. If complete path information is not provided, MDaemon will first search for the executable in the MDaemon directory, then in the Windows System directory, next in the Windows directory, and finally the directories listed in the PATH environment variable.

…suspend all operations for xx seconds

The value entered here determines how MDaemon will behave while the specified program is in progress. MDaemon can be configured to pause its execution thread for the number of seconds specified while waiting for the process thread to return. If the process returns before the number of seconds has elapsed, MDaemon will resume its execution thread immediately. Enter the numeral zero in this control and MDaemon will not suspend operations at all. Entering "-1" will cause MDaemon to wait until the process returns, no matter how long that might be.

Don't execute when queue is empty

Enable this switch if you do not want the specified program to run when the queue is empty.

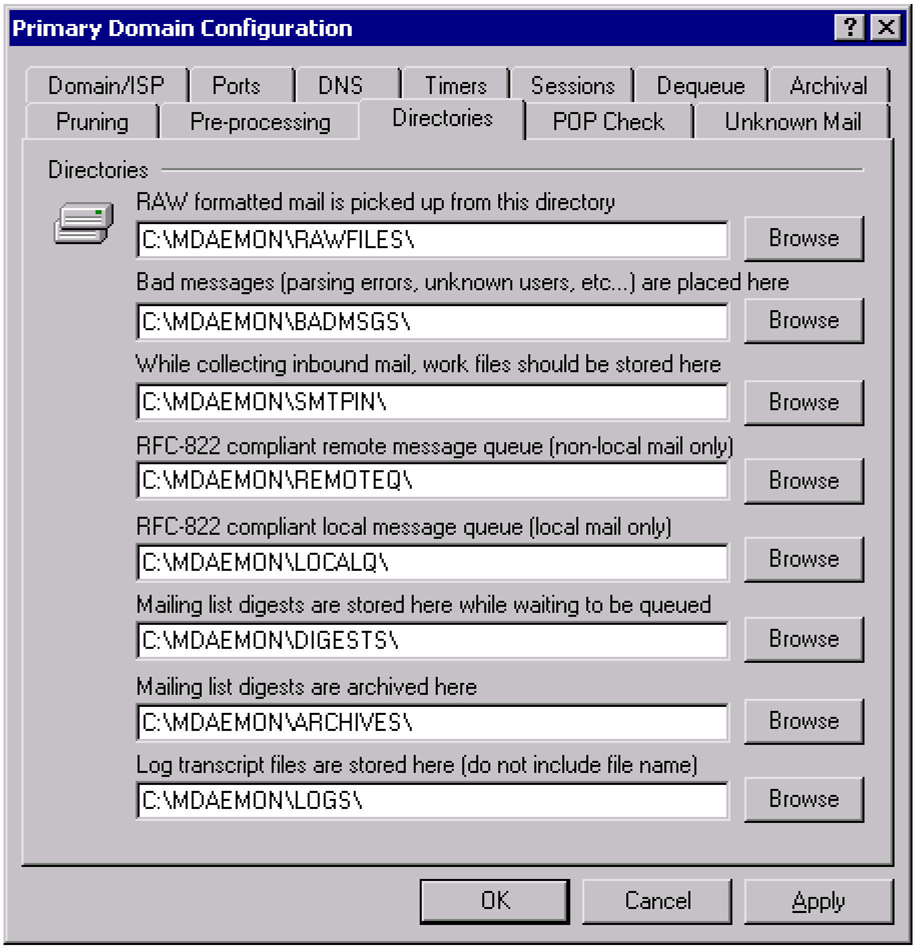
Force process to terminate

Sometimes the process you need to run may not terminate on its own. This switch will cause MDaemon to force the session to terminate once the time specified in …*Suspend All Operations For XX Seconds* has elapsed. This switch does not work if the elapsed time interval is set to "-1".

Run process in a hidden window

Click this checkbox if you want the process to run in a hidden window.

Directories



Directories

RAW formatted mail is picked up from this directory: C:\MDAEMON\RAWFILES\

Bad messages (parsing errors, unknown users, etc...) are placed here: C:\MDAEMON\BADMSGS\

While collecting inbound mail, work files should be stored here: C:\MDAEMON\SMTPIN\

RFC-822 compliant remote message queue (non-local mail only): C:\MDAEMON\REMOTEQ\

RFC-822 compliant local message queue (local mail only): C:\MDAEMON\LOCALQ\

Mailing list digests are stored here while waiting to be queued: C:\MDAEMON\DIGESTS\

Mailing list digests are archived here: C:\MDAEMON\ARCHIVES\

Log transcript files are stored here (do not include file name): C:\MDAEMON\LOGS\

Directories

RAW formatted mail is picked up from this directory

Enter the directory path where **MDaemon Server v6** should expect to find RAW format messages that are to be processed and entered into the mail stream. This directory is scanned at each local mail processing interval for RAW mail, which the server then converts to RFC-822 and delivers to its intended recipient(s).

For a complete discussion of RAW message specifications see:

The RAW Message Specifications – page 316

Bad messages (parsing errors, unknown users, etc) are placed here

Enter the directory path where bad messages should be placed. The bad message queue will contain messages destined for unknown yet supposedly local users, and messages that cause parsing problems.

When collecting inbound mail, work files should be stored here

Enter the directory path where MDaemon should store incoming transient SMTP mail messages. This work directory is used only while an SMTP session is in progress. While a session is ongoing, the messages being delivered to the server are stored in temporary files in this directory.

RFC-822 compliant remote message queue (non-local mail only)

Enter the directory path that MDaemon should use as the outbound mail queue. This directory will contain only processed RFC-822 format messages that are waiting for delivery to their final destination or to the mail gateway. All mail placed in this directory must be RFC-822 compliant and have an extension of `MSG` in order to be processed by MDaemon. Mail in this queue is destined for domains hosted by other servers.

RFC-822 compliant local message queue (local mail only)

Enter the directory path that MDaemon should use as the local mail queue. This directory will contain only processed RFC-822 format messages that are waiting for delivery to their final destination or to a mail gateway. All mail placed in this directory must be RFC-822 compliant and have an extension of `MSG` in order to be processed by MDaemon. Mail in this queue is destined for local mailboxes.

If you are using the LAN Domains feature, messages destined for other servers on your local LAN will be stored in a subdirectory of the this Local Message Queue called `Lndomain`.

See:

LAN Domains—page 148

Mailing list digests are stored here while waiting to be queued

Enter the directory path where MDaemon should store *Digest* mail waiting to be queued for delivery.

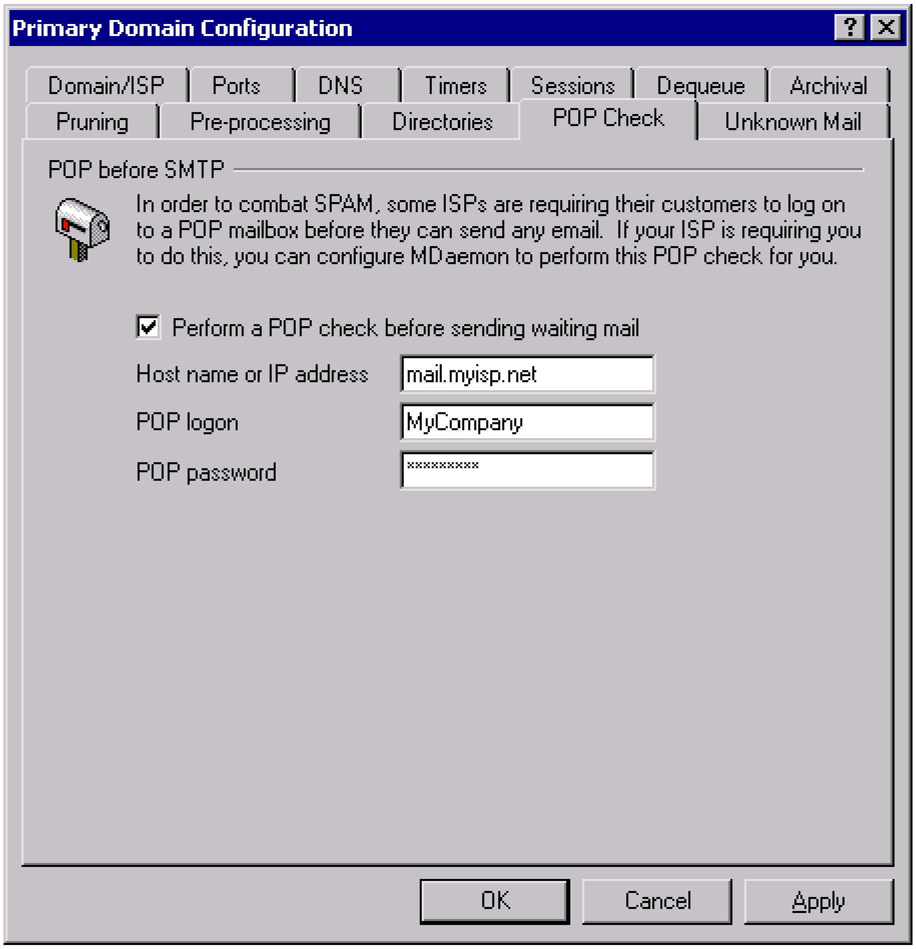
Mailing list digests are archived here

Enter the directory path where MDaemon should Archive *Digests*.

Log transcript files are stored here

Enter the directory where transaction and event logs are stored.

POP Check



Primary Domain Configuration

POP before SMTP

In order to combat SPAM, some ISPs are requiring their customers to log on to a POP mailbox before they can send any email. If your ISP is requiring you to do this, you can configure MDaemon to perform this POP check for you.

☑ Perform a POP check before sending waiting mail

Host name or IP address: mail.myisp.net

POP logon: MyCompany

POP password: **********

POP Before SMTP

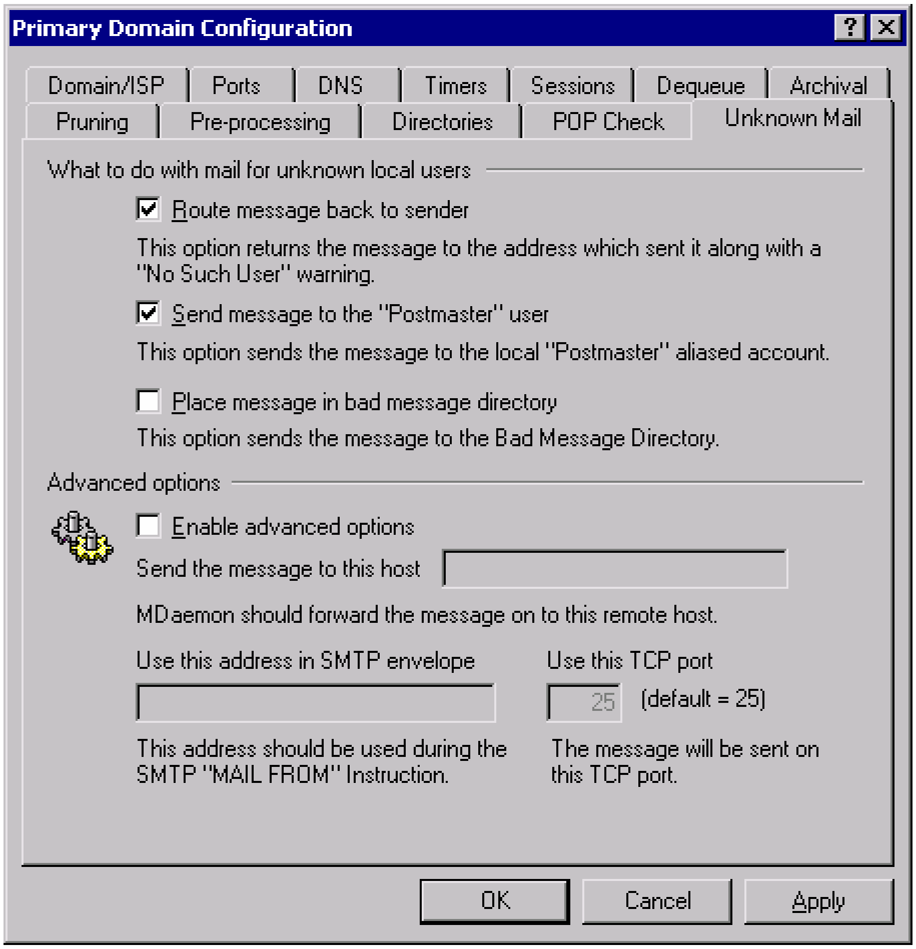
Perform a POP check before sending waiting mail
Click this checkbox if you are required to perform a POP check before sending waiting mail.

Host name or IP address
Enter the host or IP address to which you wish to connect.

POP logon
This is the POP account's logon or account name.

POP password
This is the account's POP password.

Unknown Mail



What to do with mail for unknown local users

☑ Route message back to sender

This option returns the message to the address which sent it along with a "No Such User" warning.

☑ Send message to the "Postmaster" user

This option sends the message to the local "Postmaster" aliased account.

□ Place message in bad message directory

This option sends the message to the Bad Message Directory.

Advanced options

□ Enable advanced options

Send the message to this host

MDaemon should forward the message on to this remote host.

Use this address in SMTP envelope

This address should be used during the SMTP "MAIL FROM" Instruction.

Use this TCP port: 25 (default = 25)

The message will be sent on this TCP port.

What To Do With Mail For Unknown Local Users

Route message back to sender

Messages that arrive at the server destined for unknown yet supposedly local users will be returned to the message originator if this option is activated.

Send message to the "Postmaster" user

Messages that arrive at the server destined for unknown yet supposedly local users will be forwarded to whatever user has been aliased as the postmaster.

Place message in bad message directory

Messages that arrive at the server destined for unknown yet supposedly local users will be routed to the bad message directory.

Advanced Options

Enable advanced options

Click this checkbox to enable the following advanced mail routing properties.

Send the message to this host

If a mail host is specified here, messages addressed to unknown local users will be sent to it.

Use this address in SMTP envelope

This address will be used in the SMTP "`Mail From:`" statement used during the session handshaking with the accepting host. Normally the sender of the message is used in this portion of the SMTP envelope. If you require an empty command (`MAIL FROM <>`) then enter "`[trash]`" into this control.

Use this TCP port

MDaemon will send this message on the TCP port specified here rather than the default SMTP outbound port.

Chapter

4

Secondary Domains

Hosting additional Domains with MDaemon.

Hosting Multiple Domains (MDaemon Pro only)

MDaemon Server Version 6 contains full support for multiple domains. In addition to the Primary Domain Configuration settings (page 34), it contains the Secondary Domain Editor used for designating any number of additional domains that you want to support as well as the IP address to which each will be associated. MDaemon supports both dedicated and multi-homed IP addresses.

In order to support multi-homing (sharing the same IP across multiple different domains) MDaemon automatically detects the IP address that an incoming connection is attempting to reach and uses the appropriate domain name accordingly. For example, suppose you have the following domains and accounts configured:

```
altn.com, IP = 1.1.1.1
   user-1@altn.com, logon = user-1, POP password = ALTN
arvelh.com - 2.2.2.2
   user-2@arvelh.com, logon = user-2, POP password = ARVELH
```

If a connection is attempted to 1.1.1.1 then MDaemon will answer as "altn.com". If a connection is made to 2.2.2.2 then "arvelh.com" will be used.

If `user-1@altn.com` connects to `1.1.1.1` to check his mailbox, he will supply "`user-1`" as his logon and "`ALTN`" as his password to log in. However, if `user-2@arvelh.com` connects to `1.1.1.1` to check his mail then he is technically connecting to the wrong server (he should be connecting to `2.2.2.2`). In that case, he will need to supply his full email address in the login field to gain access. Of course, if he had connected to `2.2.2.2` he would only need to supply his login value. Therefore, if an account connects to the IP address corresponding to its domain, and that IP address is not used by any other domain, then the account need only specify the login value. Otherwise, it must specify a complete email address. In this way, support for servicing multiple domains can be accomplished using a single IP address. When several domains share the same IP address then the login must contain the full email address. Otherwise MDaemon will not know which user is attempting to log in. When in doubt use the full email address as your login value.

So, how is the login and domain specified? You would expect that providing the account's email address would work like this: `arvel@altn.com`. MDaemon will always accept logon values that contain the '@' symbol, so if your mail client supports using the '@' symbol in the logon value then there is no problem. However, it turns out that many email clients on the market today will not allow the '@' symbol to be used in the login field. To accommodate those mail clients that do not permit this, MDaemon allows you to specify an alternative character. MDaemon's default alternative character is '$'. That means that you could use: `arvel$altn.com` as easily as `arvel@altn.com`.

The alternative character is specified on the System tab of the Miscellaneous Options dialog (page 203). This value can be up to 10 characters long, making it possible to provide a string of characters to serve as the delimiter instead of only a single character such as '$'. For example, using '**`.at.`**' will allow you to make logon values of "`arvel.at.altn.com`".

Several key features, such as Accounts, Mailing Lists, and Security Settings, are on a per domain basis. When you create a mail account you must specify the domain to which the new account belongs. The same goes for Mailing Lists. This means that features such as the IP Screen and IP Shield are tied to domains individually. Some features, however, such as the DomainPOP 'Real Name Matching' feature, are tied exclusively to the primary domain.

As part of the multi-domain process, when you create a secondary domain the following aliases will be set up to automatically:

```
MDaemon@secondarydomain.com = MDaemon@primarydomain.com
listserv@secondarydomain.com = MDaemon@primarydomain.com
listserver@secondarydomain.com = MDaemon@primarydomain.com
list-serv@secondarydomain.com = MDaemon@primarydomain.com
```

These aliases will be automatically removed if the secondary domain is deleted.

Secondary Domain Editor

MDaemon Server Version 6 contains full support for multiple domains. In addition to the Primary Domain Configuration settings (page 34), it contains the **Secondary Domains Editor** used for designating any number of additional domains that you wish to support as well as the IP address to which each will be associated. MDaemon supports both dedicated (static) and multi-homed IP addresses.

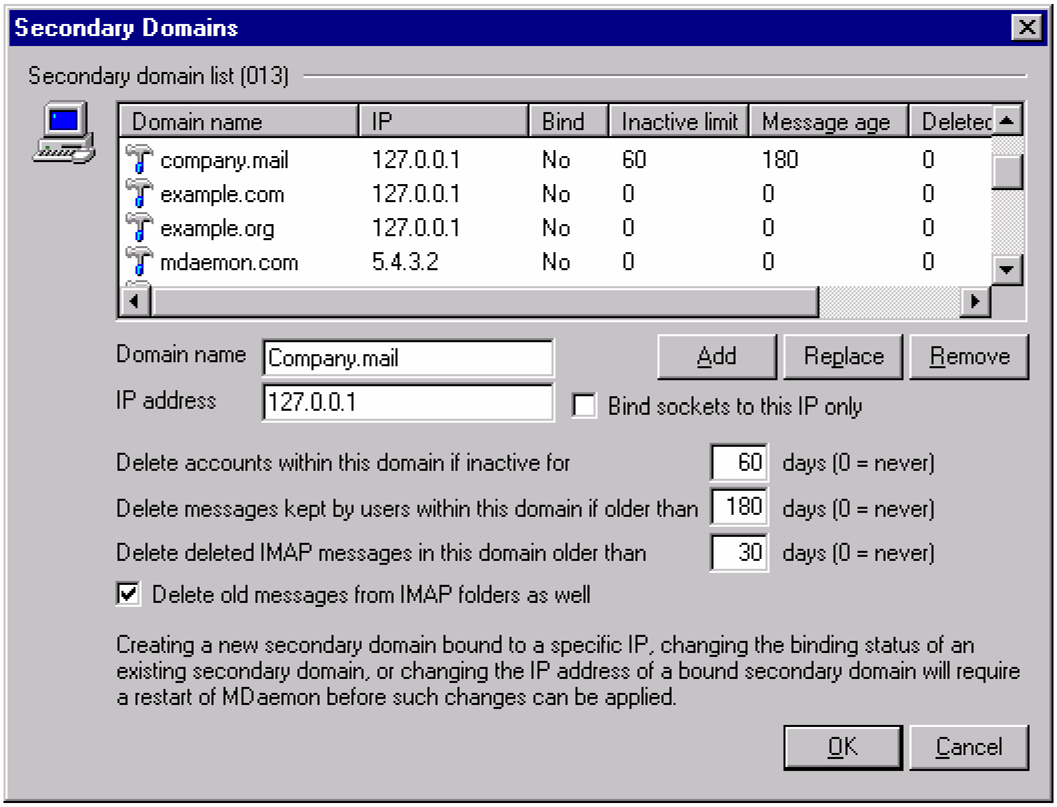
On the Secondary Domains Editor, for each secondary domain that you wish to host, you will include: the domain name, the IP address to which it will be associated, and whether or not it will be bound to its IP address.

For more information on hosting multiple domains, see:

Hosting Multiple Domains—page 62

See also:

Primary Domain Configuration—page 34
Account Editor—page 222



Secondary domain list (013)

Domain name	IP	Bind	Inactive limit	Message age	Deletec
company.mail	127.0.0.1	No	60	180	0
example.com	127.0.0.1	No	0	0	0
example.org	127.0.0.1	No	0	0	0
mdaemon.com	5.4.3.2	No	0	0	0

Domain name: Company.mail

IP address: 127.0.0.1

□ Bind sockets to this IP only

Delete accounts within this domain if inactive for 60 days (0 = never)

Delete messages kept by users within this domain if older than 180 days (0 = never)

Delete deleted IMAP messages in this domain older than 30 days (0 = never)

☑ Delete old messages from IMAP folders as well

Creating a new secondary domain bound to a specific IP, changing the binding status of an existing secondary domain, or changing the IP address of a bound secondary domain will require a restart of MDaemon before such changes can be applied.

Secondary Domain List

This window contains the list of your secondary domains. It has several columns: Domain Name—lists the name of each domain, IP—each domain's IP address, Bind—shows whether or not the given domain is bound to its IP address, and several other columns that correspond to the controls below the list. This list can be sorted in ascending or descending order by any column. Simply click the column by which you wish to sort the list and it will be sorted by that column in ascending order. Click the same column again to sort it in descending order.

Domain name

Enter the domain name of the secondary domain that you wish to host.

IP address

Enter the IP address to associate with the domain being added or edited.

Bind sockets to this IP only

Click this checkbox if you want to bind the secondary domain to its IP address.

Add

Click this button to add the secondary domain along with its IP address and binding status to the Domain List.

Replace
When you click an entry in the Domain List, its settings will appear in the corresponding controls. Click this button after making any desired changes to the information to replace the entry with the new settings.

Remove
After selecting an entry in the Domain List, click this button to remove it from the list.

Account and Old Mail Pruning

The remaining three controls on this dialog have corresponding controls on the Accounts Editor (page 230) that can be used if you want an individual account's settings to override these defaults.

Delete accounts within this domain if inactive for XX days (0=never)
Specify the number of days that you wish to allow an account belonging to this domain to be inactive before it will be deleted. A value of "0" in this control means that accounts will never be deleted due to inactivity.

Delete messages kept by users within this domain if older than XX days (0=never)
A value specified in this control is the number of days that any given message may reside in a user's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

Delete deleted IMAP messages in this domain older than XX days (0 = never)
Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this domain's users' folders. Messages flagged for deletion longer than this number of days will be purged from their mailboxes. A value of "0" means that messages flagged for deletion will never be purged due to their age.

Delete old messages from IMAP folders as well
Click this checkbox if you want the "*Delete messages kept by users…*" control to apply to messages in IMAP folders as well. When this control is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

Note

When old messages are pruned, rather than actually delete them, MDaemon will move them to the "`...\BADMSGS\[Mailbox]\`" folder where they can be manually deleted later by the administrator or a nightly process. This only applies to pruned old messages – when an account is pruned, it will be deleted along with its messages instead of moved. See `AccountPrune.txt` in the "...`MDaemon\App\`" folder for more information and command line options.

Adding a Secondary Domain

To add a secondary domain to the Domain List:

1. Enter the *Domain Name* and *IP Address*.
2. Click *Bind To This IP* (**only** if you want to bind the domain to its IP address).
3. Click *Add*.

Editing a Secondary Domain

To edit a secondary domain:

1. Click the Domain List entry that you wish to edit.
2. Make any desired changes to the information the will appear in the controls.
3. Click *Replace*.

Removing a Secondary Domain

To remove a secondary domain:

1. Click the entry that you wish to remove from the Domain List.
2. Click *Remove*.

Chapter

5

Remote Configuration

Setting up Remote Configuration. Using MDConfig and WebAdmin.

Setting up Remote Configuration

Use the **Setup|Remote Configuration…** menu selection to set up access to your server from the MDConfig remote configuration client, or from the browser-based WebAdmin server. By using these features you can review or edit any of MDaemon's controls or settings from a remote location.

The Remote Configuration dialog is used to designate whether or not MDaemon will allow remote configuration from MDConfig, WebAdmin, or both. In addition, you may assign separate logon and password values for both Administrator and Supervisor access from MDConfig, and you may designate specific IP addresses from which it will be permitted to connect to MDaemon. This effectively makes it possible to permit remote configuration access from only specific machines. Finally, you may specify a directory in which MDaemon will place a backup of its existing configuration files before it updates any changes that you make.

Note

WebAdmin is not installed by default with the MDaemon server. It is a free plug-in that can be obtained from Alt-N Technologies at www.altn.com.

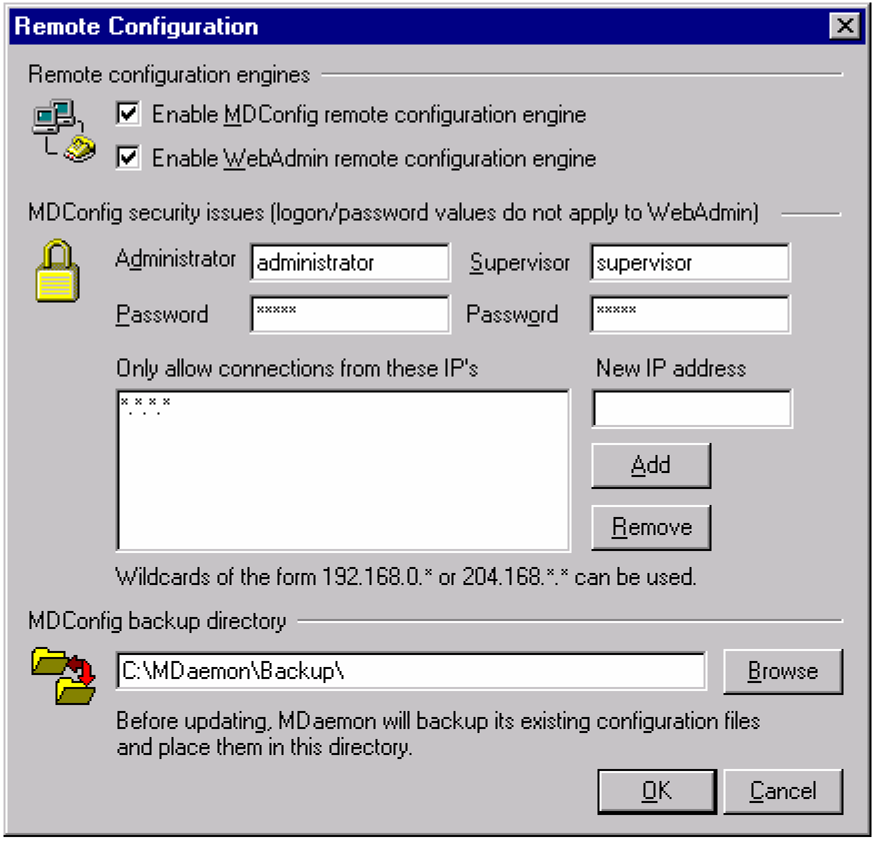
For more information regarding MDConfig and WebAdmin, see:

MDConfig Remote Configuration Client—page 70
Web Access Defaults—page 218
Account Editor|Web—page 234

WebAdmin – Remote Server Administration

For complete information on WebAdmin, see the **WebAdmin User Manual**. You can obtain the manual from www.altn.com.

Remote Configuration



Remote Configuration

Remote configuration engines

☑ Enable MDConfig remote configuration engine

☑ Enable WebAdmin remote configuration engine

MDConfig security issues (logon/password values do not apply to WebAdmin)

Administrator: administrator Supervisor: supervisor

Password: ***** Password: *****

Only allow connections from these IP's: *.*.*.*

New IP address:

Wildcards of the form 192.168.0.* or 204.168.*.* can be used.

MDConfig backup directory

C:\MDaemon\Backup\

Before updating, MDaemon will backup its existing configuration files and place them in this directory.

Remote Configuration Engines

Enable MDConfig remote configuration engine

Click this Checkbox to enable support for remote configuration. MDaemon will listen for connections on the MDConfig port specified on the Domain Configuration Editor (page 41). When this switch is cleared, all attempts to remotely configure the server using MDConfig will fail. The MDConfig server can also be enabled/disabled from the Message Router.

Enable WebAdmin remote configuration engine

Click this checkbox if you want to enable MDaemon's WebAdmin server. With this server active, MDaemon's files can be edited using a web browser by connecting to MDaemon's primary domain URL and specifying the port on which WebAdmin is listening (page 41). For example: if your primary domain's URL was "www.altn.com" and WebAdmin was listening on port 1000, then you could reach WebAdmin by pointing your browser to "http://www.altn.com:1000". The WebAdmin server can also be enabled or disabled from the Message Router.

MDConfig Security Issues (these do not apply to WebAdmin)

Administrator

MDConfig must send this logon and its accompanying password in order to gain administrator access to the remote configuration process. This level of access permits changes to every configuration aspect of MDaemon.

Password

This password must be provided along with the Administrator logon in order to gain administrator access to remote configuration.

Supervisor

When this logon with its accompanying password is sent by MDConfig, supervisor access to remote configuration will be granted. This level of access permits changes to accounts and account related functions within MDaemon such as auto-responders, account aliases, and account settings.

Password

This password must accompany the Supervisor Name in order for the client to gain supervisor level access to remote configuration.

Only allow connections from these IPs

The IP addresses listed here are the only ones from which MDaemon will accept a remote configuration connection. Wildcards are permitted.

New IP address

To add an IP address from which you wish to allow Remote Configuration, enter the IP address here and then click the *Add* button.

Add

Click this button to add an IP Address that you have entered into the *New IP Address* text box.

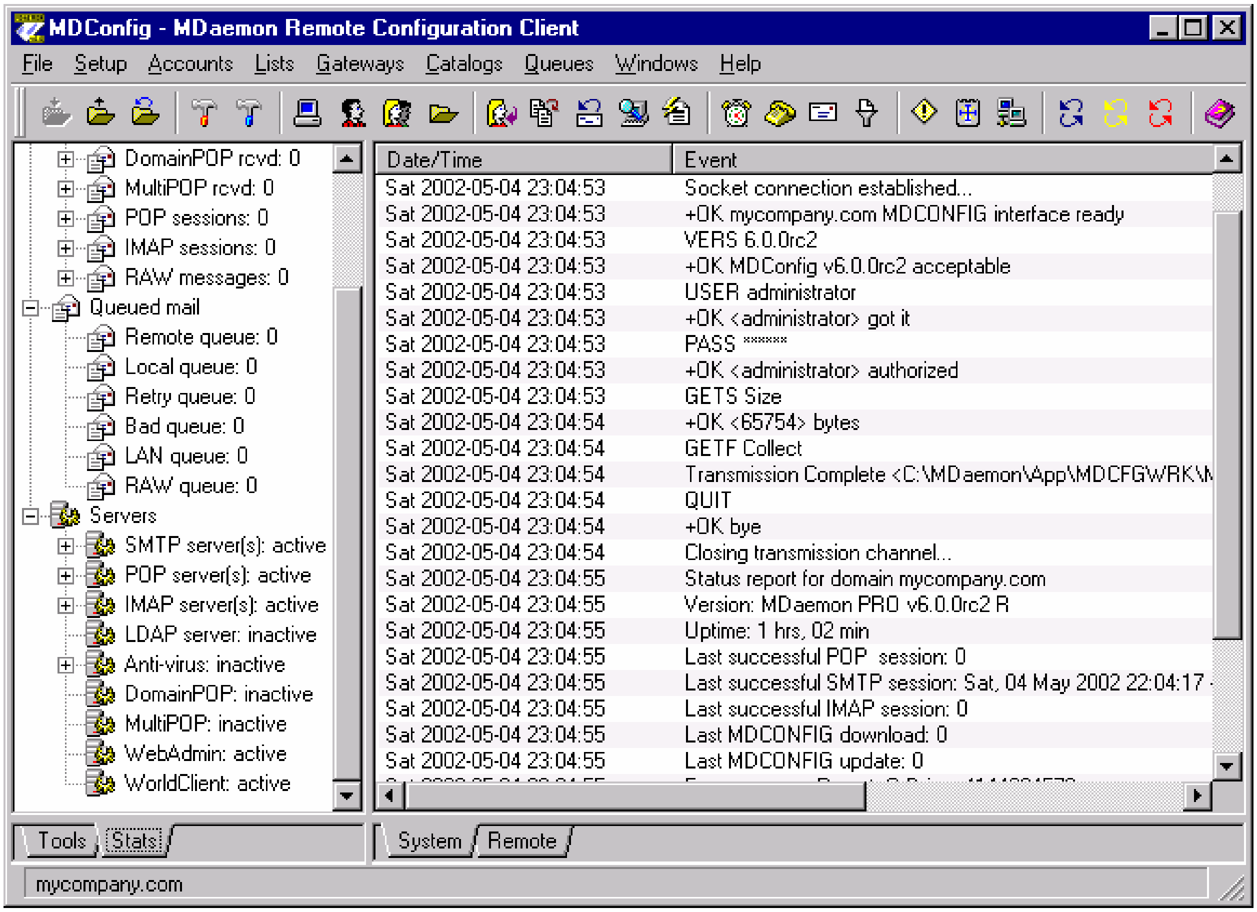
Remove

Click this button to remove a selected IP address from the display window.

MDConfig Backup directory

If specified, MDaemon will backup original copies of updated configuration files to this directory.

MDConfig - Remote Configuration Client



```
DomainPOP rcvd: 0
MultiPOP rcvd: 0
POP sessions: 0
IMAP sessions: 0
RAW messages: 0
Queued mail
    Remote queue: 0
    Local queue: 0
    Retry queue: 0
    Bad queue: 0
    LAN queue: 0
    RAW queue: 0
Servers
    SMTP server(s): active
    POP server(s): active
    IMAP server(s): active
    LDAP server: inactive
    Anti-virus: inactive
    DomainPOP: inactive
    MultiPOP: inactive
    WebAdmin: active
    WorldClient: active
```

```
Date/Time                 Event
Sat 2002-05-04 23:04:53   Socket connection established...
Sat 2002-05-04 23:04:53   +OK mycompany.com MDCONFIG interface ready
Sat 2002-05-04 23:04:53   VERS 6.0.0rc2
Sat 2002-05-04 23:04:53   +OK MDConfig v6.0.0rc2 acceptable
Sat 2002-05-04 23:04:53   USER administrator
Sat 2002-05-04 23:04:53   +OK <administrator> got it
Sat 2002-05-04 23:04:53   PASS ******
Sat 2002-05-04 23:04:53   +OK <administrator> authorized
Sat 2002-05-04 23:04:53   GETS Size
Sat 2002-05-04 23:04:54   +OK <65754> bytes
Sat 2002-05-04 23:04:54   GETF Collect
Sat 2002-05-04 23:04:54   Transmission Complete <C:\MDaemon\App\MDCFGWRK\M
Sat 2002-05-04 23:04:54   QUIT
Sat 2002-05-04 23:04:54   +OK bye
Sat 2002-05-04 23:04:54   Closing transmission channel...
Sat 2002-05-04 23:04:55   Status report for domain mycompany.com
Sat 2002-05-04 23:04:55   Version: MDaemon PRO v6.0.0rc2 R
Sat 2002-05-04 23:04:55   Uptime: 1 hrs, 02 min
Sat 2002-05-04 23:04:55   Last successful POP  session: 0
Sat 2002-05-04 23:04:55   Last successful SMTP session: Sat, 04 May 2002 22:04:17 -
Sat 2002-05-04 23:04:55   Last successful IMAP session: 0
Sat 2002-05-04 23:04:55   Last MDCONFIG download: 0
Sat 2002-05-04 23:04:55   Last MDCONFIG update: 0
```

mycompany.com

Introduction

The capability to remotely control MDaemon's configuration parameters is fully supported using the MDConfig Remote Configuration Client. Utilizing a POP3-like proprietary protocol, a method exists whereby a client package such as MDConfig can connect to a running instance of MDaemon Server and mimic its configuration and setup. This makes it possible for MDConfig to alter the setup parameters of the host MDaemon. Once the desired configuration changes have been made, MDConfig reestablishes contact with the remote MDaemon site and uploads all the new changes, which will take effect immediately.

The steps involved are straightforward. A connection is made to a remote site that is running MDaemon. MDConfig and MDaemon exchange handshaking information, which includes a username and password for security (see **Remote Configuration**—page 68). Once the handshaking session is complete, the host MDaemon sends all of its configuration information and files to the remote MDConfig client. At this point MDConfig mimics the host MDaemon's settings using all the familiar dialog boxes, buttons, and controls that users have come to expect when configuring MDaemon. Finally, after making any desired changes to MDaemon's settings, MDConfig uploads all of the changes to the remote MDaemon site where they will be implemented.

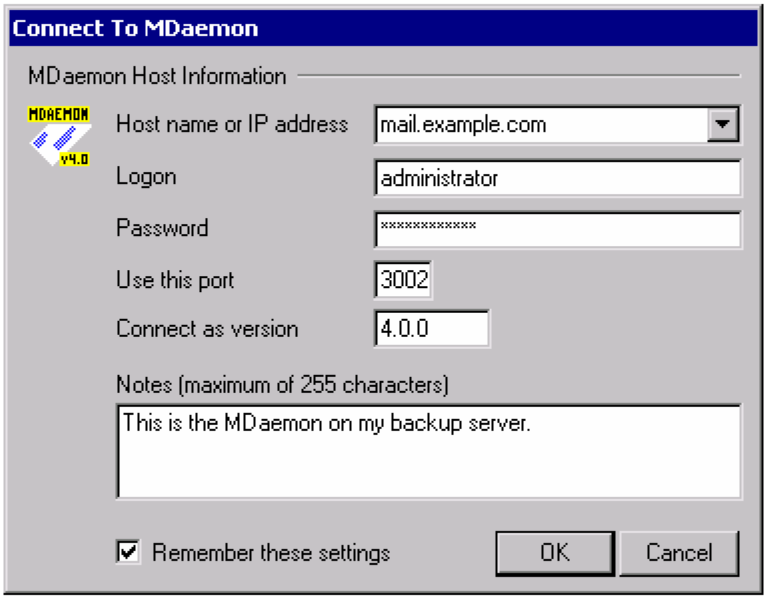
Only one site can be remotely configured at a time. Once configuration information is provided from a remote site to MDConfig, it is not possible to gather configuration information from another site until the existing configuration session has been reset (see ***Resetting MDConfig For A New Connection*** below). In addition, it is very important to realize that changes to a site's configuration information do not take effect until the changes are uploaded to the remote site (see ***Updating The Remote MDaemon Site*** below). Further, if changes are made to the remote site's configuration using the primary MDaemon interface while an MDConfig session is underway, those changes will not be reflected in the configuration information gathered by MDConfig at the start of the session and are likely to be overwritten when MDConfig updates the remote site. For this reason you must avoid making changes to MDaemon locally while it is being configured using MDConfig.

Instructions for moving MDConfig to another computer on your network are listed at the end of this Section.

Connecting to a Remote MDaemon Site

File | Connect…

This menu selection, or toolbar button, opens the Connect to MDaemon dialog on which you will specify the connection and security information needed to connect to MDaemon.



Connect To MDaemon

MDaemon Host Information

Host name or IP address: mail.example.com

Logon: administrator

Password: ************

Use this port: 3002

Connect as version: 4.0.0

Notes (maximum of 255 characters): This is the MDaemon on my backup server.

☑ Remember these settings

For a remote configuration session to be established, the remote MDaemon site's **Remote Configuration** settings (page 68) must match those supplied on this dialog.

Server Information

Host name or IP address
Enter the domain name or IP address of the MDaemon site to which you wish to establish a remote configuration session. This control's drop-down list box will contain entries for each host name or IP address that was used when the "Remember these settings" control was enabled. When one of those entries is selected the rest of the controls on this dialog will display the corresponding information for that entry.

Logon

The value entered here must match the Administrator or Supervisor Name setting found on MDaemon's Remote Configuration dialog.

Password

The value entered here must match the Password corresponding to the Logon being used. This setting is also found on MDaemon's Remote Configuration dialog.

Use this port

Enter the port on which you have configured MDaemon to listen for MDConfig connections.

Connect as version

If you are connecting to an earlier version of MDaemon, use this control to specify that version.

Notes (maximum of 255 characters)

This text box can be used to display notes or descriptions related to each MDaemon server to which you connect. Its contents will correspond to whichever entry you have selected in the "Host name or IP address" control. For example, if you use MDConfig to manage MDaemon installations on multiple servers with similar IP Addresses then you can type a description of each server in this box to help you remember which is which. That way when you select a particular entry its description will appear in this area. The notes for an entry will only be saved when the "Remember these settings" control is enabled and you have clicked the "OK" button.

Remember these settings

Clear this checkbox if you do not want the current entry's settings to be retained for later use. When this control is enabled then all information corresponding to the currently displayed "Host name or IP address" will be saved along with any previously saved entries.

Updating the Remote MDaemon Site

File | Update

Once you have finished modifying any MDaemon configuration parameters, choose this menu selection, or its corresponding button on the toolbar, to upload your modifications to the remote site. Since only one host can be configured at a time, pressing this button updates the last host from which configuration information was gathered.

Clearing Alterations without Updating the Remote Site
Resetting MDConfig for a New Connection

File | Reset

This function clears the workspace and prepares MDConfig to connect to a new remote MDaemon site. Any MDaemon settings currently displayed in MDConfig's interface will be erased. Therefore, take care to update any changes to the remote site before resetting unless you wish to abort your configuration changes. Downloading MDaemon's configuration and then Resetting or closing MDConfig without uploading the changes will in no way affect MDaemon nor alter any MDaemon settings.

Moving MDConfig to Another Computer

Use MDaemon's executable installation file to install only MDConfig on the remote machine. Simply proceed through the normal MDaemon installation process but enable only the MDConfig installation option when asked which items to install.

Alternatively, you can copy the necessary files from your current installation and manually move them to the other machine. To do that, copy these files into their own directory on the other computer:

`CFEngine.exe`
`CFilter.dll`
`CFilter.exe`
`MDCONFIG.EXE,`
`MDUSER.DLL,`
`MDUserLdap.dll`
`NTUtil.DLL, and`
`XCeedZip.DLL` files into their own directory on the other computer.

Further, MDConfig uses CTL3D and Borland Custom Control DLL files. These files were installed along with MDConfig on the original computer. The files you need are `CTL3D*.DLL` and `BWCC*.DLL` from the original computer's Windows System directory. They need to be placed into the new computer's Windows System directory, not in the same directory as `MDCONFIG.EXE` and `MDUSER.DLL`. For Windows 95 systems, the directory is `\windows\system`. For NT4 machines it is `\windows\system32`.

Chapter

6

WorldClient Server

Setting up and using the WorldClient Server

Overview

Included in MDaemon v6 is WorldClient. WorldClient is a web-based email solution designed to offer users email client functionality using their favorite web browser. All of their email folders reside on the server so that they have access to everything as if they were at the office. WorldClient can easily hold its own against traditional mail clients while providing the added bonus of its ability to enable users to access their email from anywhere at anytime.

There are many ways in which WorldClient can be used. Use it to keep your mobile staff in touch with their email—remember, WorldClient is not workstation dependent so "mobile" can also mean just traveling across the building. Use WorldClient to offer web-based email services to your customers, and customize the interface to display advertising banners. Use it on a kiosk or in a computer lab to provide email to students or other individuals who may not have a personal computer of their own.

WorldClient also provides many benefits to email administrators. Now you don't have to configure and maintain each individual email client since WorldClient isn't workstation dependent. Customize the graphical images and HTML pages used in WorldClient to suit your corporate needs or the needs of your customer. Further, give your users the ability to maintain their own account settings thus saving you time—you can give as much or as little control to your users as you want.

Finally, there are features that will benefit your customers directly, such as: extensive email functionality wherever you find a browser, client-side interface available in 18 languages, personal and global address books, manageable mail folders and filters, send/receive file attachments, multiple visual "themes" for interface, and much more.

Calendar & Scheduling System

New to WorldClient in MDaemon 6.0 is a complete calendar and event scheduling system. The Calendar System can be used to post memorandums and schedule and review appointments and meetings, both for you and for your domain's users. Appointments and meetings can be designated as public or private, giving you complete control over which users, if any, are allowed to see them. By simply selecting a user's name from a drop-down list, you can see that user's calendar and review all events to which you have been giving access. If you have been giving write-access permission to that user's calendar, you can even schedule events for them.

Because the Calendar system is integrated with MDaemon, there is the added benefit of email notifications of meetings and third-party scheduled appointments. Whenever someone other than yourself schedules an appointment for you, you will receive an email message summarizing the appointment. For meetings, each designated meeting attendee will receive an email message detailing the meeting's date, time, location, subject, and list of attendees. Further, any attendees who have calendar entries that conflicted with the meeting's timeslot will receive a message notifying them of the meeting and its conflict with their schedule. The person who scheduled the meeting will receive a summary message listing all of the meeting's details and invited attendees who did or did not have scheduling conflicts. Finally, using the Calendar's Auto-scheduling feature, conflicts can be avoided altogether by allowing the calendar system to search for the first available timeslot with no scheduling conflicts. Then you can either accept the suggested timeslot or choose a new one.

WorldClient is also equipped with support for Internet Calendar (iCal) used by Microsoft Outlook and other iCalendar compliant email programs. WorldClient can detect and process iCalendar information sent to your users and update their calendars accordingly. When a user opens an iCalendar attachment from within WorldClient the information contained in the attachment will be reflected in the users WorldClient calendar. Also, when users create new meetings or appointments they can list one or more email addresses to whom they wish an iCalendar email to be sent. This feature can be set on a per-domain basis and then over-ridden by individual users in their WorldClient Options.

The Calendar System can also be used to post Global Memos (memorandums that will appear on everyone's calendar). This feature can be used to post a notice to an entire domain's group of users by simply creating a memo normally and then clicking a single checkbox. In addition, for added security and versatility, permission to create or see global memos can be controlled completely from within MDaemon. These controls are located on the Calendar & Scheduling tab of the WorldClient/RelayFax Properties dialog (Setup→WorldClient/RelayFax...→Calendar & Scheduling). You can grant read or write permission to all domain users, no one, or specific individuals, whatever you prefer. These permissions are all controlled on a per domain basis.

Besides controlling Global Memo permissions, the Calendar & Scheduling tab can also be used to enable and disable the Calendar System completely, for each separate domain. Thus, you can provide the group calendar features to as many or few of your hosted domains as you please.

ComAgent

Replacing WCWatch in MDaemon 6.0 is ComAgent, a secure instant messaging system, address book client, and tray applet that provides quick access to WorldClient's email features. ComAgent can be downloaded by each WorldClient user and then installed on the individual's local computer. It is preconfigured for the specific user when downloaded thus limiting the need to configure it manually.

ComAgent runs in the background and checks your account for new mail by querying the WorldClient server directly. This eliminates the need to open a browser or keep one open to check your email—ComAgent checks for new mail and notifies you with a sound or visual alert when new mail arrives. ComAgent also displays a list of your mail folders and the number and type of messages that each one contains (new, unread, and read). Furthermore, it can be used to launch your browser and move it immediately to a specific mail folder, the first unread message, the compose page, or your calendar page.

Additionally, when you are using Alt-N's "LDaemon" LDAP server to maintain WorldClient's Public and Private address books, ComAgent can be used to provide two-way synchronization between LDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

Finally, ComAgent is also equipped with a complete instant messaging system. You can view your list of ComAgent "buddies" and each one's online status (online, away, offline), start a conversation with any one or group of them, set your own online status, and view past conversations in a history folder. For specific instructions on how to use ComAgent, see its online help system.

There are several options related to ComAgent and instant messaging (IM) located on the Domain Options tab—page 81.

ComAgent's Instant Messaging System

ComAgent is equipped with a simple but effective instant messaging (IM) system. With this system you can communicate instantly with any other account on your MDaemon server. You can choose a list of "buddies" from a list of all MDaemon users and then see which ones are online and ready to receive an IM. You will also be able to start a group conversation involving several buddies at once. All of the IM features are available via the shortcut (right-click) menu within ComAgent.

ComAgent's IM system is also scriptable, which allows custom programs to interface with it. By creating semaphore (SEM) files in the **\MDaemon\WorldClient\** directory, an external application can send IM messages to ComAgent users immediately. The following is the format of the SEM file:

```
To: frank@example.com       Email address of ComAgent user.
From: rip@example.com       Email address of instant message's sender.
<blank line>
Text of instant message.    This is the text sent as an instant message.
```

The SEM file name must start with the characters "IM-" and be followed by a unique numerical value. For example, "IM-0001.SEM". Applications should also create a corresponding file called "IM-0001.LCK" to lock the SEM file. Once the SEM file is completed remove the LCK file and the SEM file will be processed. MDaemon uses this scripting method to send Instant Message reminders to you about upcoming appointments and meetings.

An action was added to the Content Filter system that uses this scripting method to send instant messages. Further, rules utilizing this action can use the Content Filter macros in the IM. For example, you can create an instant message rule that looks like this:

```
You have received an email from $SENDER$.
Subject: $SUBJECT$
```

This rule would be an effective way to get new mail alerts through ComAgent.

Because many businesses and administrators have reservations about using an Instant Messaging system in their company due to the inherent lack of centralized accountability and the inability to monitor IM traffic that is in traditional and well known IM clients, we have designed ComAgent's instant messaging system to minimize those deficiencies. First of all, our system is not peer-to-peer—individual ComAgent clients do not connect directly to each other. Further, because every IM passes through the server, each message is logged in a central location accessible to the MDaemon/WorldClient administrator. Thus a record of all conversations can be maintained for the security of both your company and your employees or users. IM activity is logged in a file called InstantMessaging.log located in the MDaemon\LOGS\ directory. The assurance of accountability is also the primary reason we do not support other IM clients such as ICQ, AOL, and MSN. We may, however, add that capability as an optional feature in some future version of MDaemon. Finally, our IM system is secure in that each transaction is strongly encrypted from start to finish so that plain text is never transmitted.

Instant Messaging is provided on a per-domain basis. Controls for activating instant messaging and designating whether or not IM traffic should be logged are located on the Server Options tab of WorldClient/RelayFax Properties (**Setup→WorldClient/RelayFax…→Server Options**).

Using WorldClient

Starting WorldClient

There are three ways to start/stop the WorldClient server:

1. On the Stats tab on the left-hand side of the Message Router, right-click on the **WorldClient** entry and choose the *Toggle Active/Inactive* selection on the shortcut menu.
2. Click **File→Enable WorldClient server** on the Message Router.
3. Click **Setup→WorldClient/RelayFax…** on the Message Router, and then click *Enable WorldClient Server* on the Server Options tab.

Logging in to WorldClient

1. Point your web-browser to `http://main-or-second-domain.com:WCPortNumber`. This port is designated on the Server Options tab of the "WorldClient/RelayFax…" dialog (page 78). If you configure WorldClient to listen to the default web port (port 80) then you do not need to denote the port number in the login URL (e.g. www.mydomain.com instead of www.mydomain.com:3000).
2. Type your MDaemon account's user name and password.
3. Click **Sign in**.

Changing WorldClient's Port Setting

1. Click **Setup→WorldClient/RelayFax…** on the Message Router.
2. Type the desired port number in the control labeled *Run WorldClient Server using this TCP Port.*
3. Click OK.

WorldClient Documentation

Client-side Help

WorldClient is equipped with extensive client-side help for your users. See the online help system within WorldClient for information on the client features and functions.

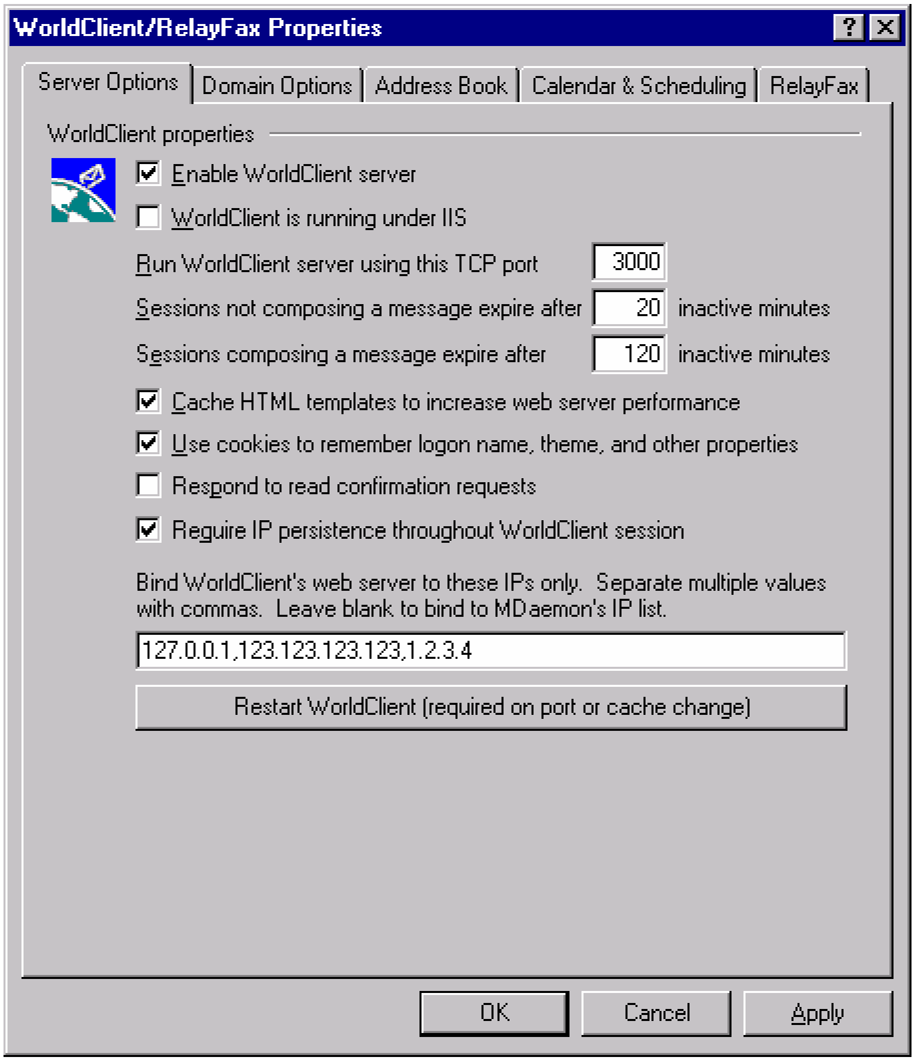
WorldClient User Manual and Help

For complete information on WorldClient see the WorldClient User Manual, and the client's online help system. You can download the manual and other helpful documentation from Alt-N Technologies' web site at **www.altn.com**.

WorldClient/RelayFax Properties

Use the **Setup→WorldClient/RelayFax…** menu selection to enable your WorldClient server and configure various WorldClient related settings. You can designate the port on which it will operate as well as the time that you wish to allow WorldClient sessions to remain inactive before they expire. You can also control many global or domain specific settings such as: the default language and theme to use, whether users can create accounts, the default pagination of the message listing, whether or not ComAgent support is enabled, whether or not Instant Messaging is allowed and logged, many Calendar and Scheduling features, Public and Private address book settings, RelayFax integration, and much more.

Server Options



WorldClient/RelayFax Properties

WorldClient properties

☑ Enable WorldClient server

☐ WorldClient is running under IIS

Run WorldClient server using this TCP port: 3000

Sessions not composing a message expire after 20 inactive minutes

Sessions composing a message expire after 120 inactive minutes

☑ Cache HTML templates to increase web server performance

☑ Use cookies to remember logon name, theme, and other properties

☐ Respond to read confirmation requests

☑ Require IP persistence throughout WorldClient session

Bind WorldClient's web server to these IPs only. Separate multiple values with commas. Leave blank to bind to MDaemon's IP list.

127.0.0.1,123.123.123.123,1.2.3.4

This tab contains various global, server level settings that govern WorldClient's configuration and behavior regardless of the users or domains to which they belong.

WorldClient Properties

Enable WorldClient server
Click this checkbox to enable the WorldClient server. You may also enable/disable WorldClient from the File menu or Statistics and Shortcuts frame of the Message Router.

WorldClient is running under IIS
When running WorldClient under Internet Information Server (IIS) rather than WorldClient's built-in web server, click this checkbox. This prevents certain GUI elements from being accessed which might otherwise cause conflicts with IIS.

For more information, see *Running WorldClient under IIS*—page 80.

Run WorldClient server using this TCP port
This is the port on which WorldClient will listen for connections from your users' web browsers.

Sessions not composing a message expire after xx inactive minutes
When a user is logged in to WorldClient but is not composing a message, this is the amount of time that their session will remain inactive before WorldClient will close it.

Sessions composing a message expire after xx inactive minutes
This timer governs how long a user's session will be kept open while they are composing a message and the session remains inactive. It is a good idea to set this timer higher than the *Sessions not composing a message…* timer since inactivity time is typically greater while a user is composing a message. This is because composing a message requires no communication with the server until the message is sent.

Cache HTML templates to increase web server performance
Click this box to cause WorldClient to cache templates in memory rather than read them each time they need to be accessed. This can dramatically increase server performance but WorldClient will have to be restarted if you ever make a change to one of the template files.

Use cookies to remember logon name, theme, and other properties
Click this option if you want WorldClient to store each user's logon name, theme, and certain other properties in a cookie on his or her local computer. Using this feature gives your users a more "customized" login experience but requires that they have support for cookies enabled in their browsers.

Respond to read confirmation requests
Click this option if you want WorldClient to respond to incoming messages that contain a request for read confirmation. When the WorldClient user opens the message MDaemon will send a notification to the sender indicating that it was displayed by the recipient. The WorldClient user who received the message will not have seen any indication that the read confirmation was requested or responded to.

Clear the check box if you want WorldClient to ignore read confirmation requests regardless of whether the message is read or not.

Require IP persistence throughout WorldClient session
As an added security measure you can click this checkbox to cause WorldClient to restrict each user session to the IP address from which the user connected when the session began. Thus, no one can "steal" the user's session since IP persistence is required. This configuration is more secure but could

cause problems for users who may be using a proxy server or dial-up account that dynamically assigns and changes IP addresses.

Bind WorldClient's web server to these IPs only

If you wish to restrict the WorldClient server to only certain IP addresses then specify those addresses here separated by commas. If you leave this field blank then WorldClient will monitor all IP Addresses that you have designated for your Primary and Secondary Domains.

Restart WorldClient (required to recognize new TCP port)

Click this button if you wish to restart the WorldClient server. Note: when changing WorldClient's port setting you must restart WorldClient in order for the new setting to be recognized.

Running WorldClient under IIS

WorldClient is equipped with a built-in web server and therefore doesn't require Internet Information Server (IIS) to operate. However, in MDaemon 6.0 IIS support has been added to WorldClient, thus it can now function as an ISAPI DLL. To configure WorldClient to operate under IIS:

1. Stop WorldClient. WorldClient cannot run using the included web server and in IIS at the same time.

2. Create a web site or virtual directory in IIS for the `\WorldClient\HTML` directory

3. Enable "Scripts and executables" permission and set `WorldClient.dll` as the default document.

4. Using Windows Explorer, give Full Control access to your MDaemon directory to the `IWAM_ComputerName` account.

5. If you have any email accounts that use NT domain authentication, edit your Local Security Policy to give `IWAM_ComputerName` the "Act as part of the operating system" user right.

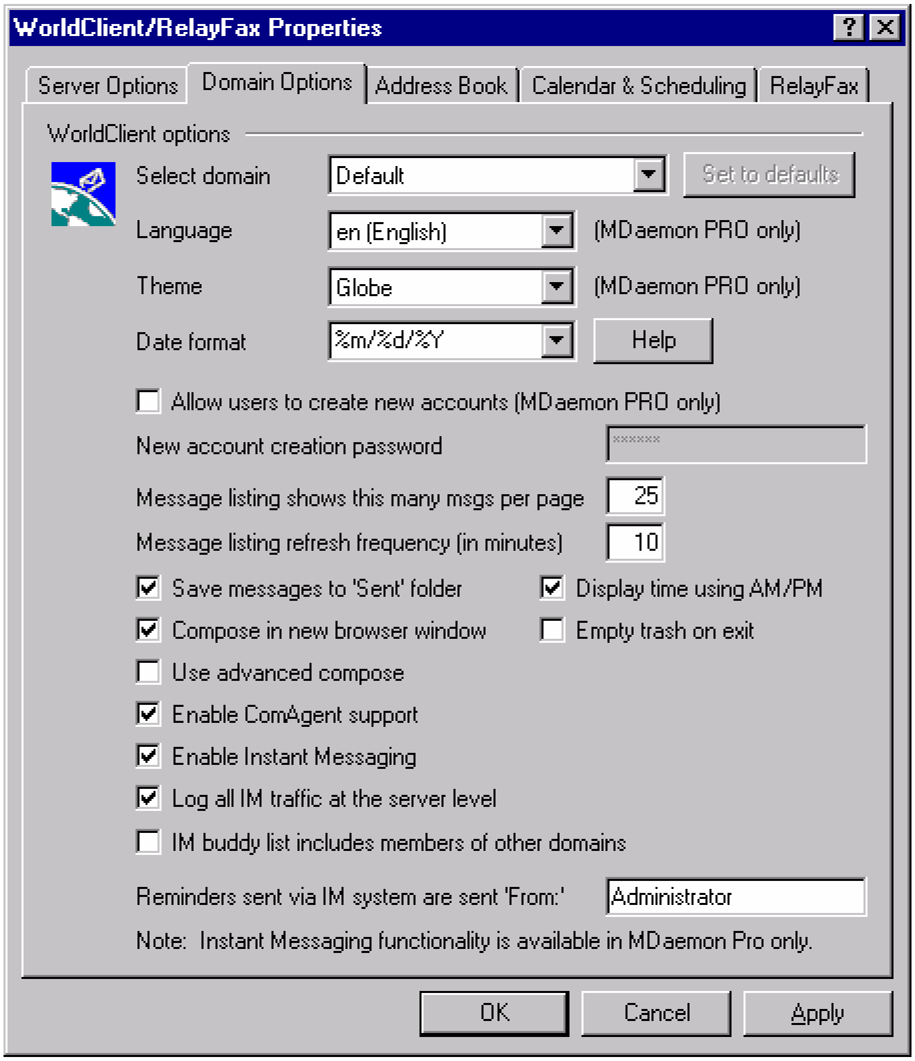
6. If you are also running WebAdmin under IIS, edit WorldClient's `Domains.ini` (located in `\MDaemon\WorldClient\`) and set the `WebAdminURL` key in the `[Default:Settings]` section to the URL of WebAdmin.

7. In MDaemon, go to **Setup→WorldClient/RelayFax…→Server Options**, and then click **WorldClient is running under IIS**.

Note

When running WorldClient under IIS you will no longer be able to start and stop it from MDaemon's interface. You must use the tools provided with IIS to do so.

Domain Options



WorldClient options

Select domain: Default

Language: en (English) (MDaemon PRO only)

Theme: Globe (MDaemon PRO only)

Date format: %m/%d/%Y

□ Allow users to create new accounts (MDaemon PRO only)

New account creation password: ******

Message listing shows this many msgs per page: 25

Message listing refresh frequency (in minutes): 10

☑ Save messages to 'Sent' folder

☑ Display time using AM/PM

☑ Compose in new browser window

□ Empty trash on exit

□ Use advanced compose

☑ Enable ComAgent support

☑ Enable Instant Messaging

☑ Log all IM traffic at the server level

□ IM buddy list includes members of other domains

Reminders sent via IM system are sent 'From:' Administrator

Note: Instant Messaging functionality is available in MDaemon Pro only.

The settings on this tab are domain specific. Most of the features and controls deal with client level behavior rather than the overall behavior and configuration of the WorldClient server.

WorldClient Options

Select domain

Use this drop-down list to choose the domain whose settings you wish to edit. Leave it set to *Default* if you wish to edit the default settings. The default settings will be used for all domains whose settings you haven't specifically changed. If you make changes to any of the settings on this tab then you must *Apply* them before switching to a different *Select domain* setting. If you make changes and then attempt to select a different domain without first applying them, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

Set to defaults

This option resets a domain to the *Default* settings. Use the *Select domain* control to select a domain and then click *Set to defaults* to restore it.

Language (MDaemon PRO only)

Use the drop-down list box to choose the default language in which the WorldClient interface will appear when your users first sign in to the selected domain. Users can change their personal language setting through an option in Options→Personalize within WorldClient.

Theme (MDaemon PRO only)

Use this drop-down list box to designate the default WorldClient theme to use for the client interface when the selected domain's users first sign in. The users can personalize the theme setting from the Options→Personalize page within the client.

Date format

Use this text box to designate how dates will be formatted for the selected domain. Click the Help button to display a list of macro codes that can be used in this text box. You can use the following macros in this control:

%A — Full weekday name

%B — Full month name

%d — Day of month (displays as "01-31")

%m — Month (displays as "01-12")

%y — 2-digit year

%Y — 4-digit year

For example, "`%m/%d/%Y`" might be displayed in WorldClient as "`12/25/2002`".

Note

This setting is per domain. Individual users cannot modify the date format used for their accounts.

Help

Click this button to display the list of macro codes that can be used in the *Date format* above.

Allow users to create new accounts (MDaemon PRO only)

Click this checkbox if you want a "Create Account" button to appear on WorldClient's sign-in screen when a user connects to the selected domain. This will enable users to create their own MDaemon accounts accessible via WorldClient.

TIP!

If you choose to allow users to create their own email accounts then you should carefully review the New Account Defaults settings (page 216). Use New Account Defaults to designate the degree of control that you will allow users to have over their own accounts.

New Account creation password

Type a password here if you want to restrict new account creation from the sign-in screen to only those users who know the password. Users will have to type the new account creation password into the Password box on the sign-in screen before the "Create Account" button will allow them to proceed. If *Create Account* is clicked without specifying the proper password, a message will be displayed stating that the password is required.

When the user is taken to the Account Creation screen they must specify their account name (mailbox name), password, full name, and the language in which they want the interface to appear.

Message listing shows this many msgs per page

This is the number of messages that will be listed on each page of the Message Listing for each of your mail folders. If a folder contains more than this number of messages then there will be controls above and below the listing that will allow you to move to the other pages. Individual users can modify this setting from the Options→Personalize page within WorldClient.

Message listing refresh frequency (in minutes)

This is the number of minutes that WorldClient will wait before automatically refreshing the Message Listing. Individual users can modify this setting from the Options→Personalize page within WorldClient.

Save messages to 'Sent' folder

Click this option if you want a copy of each message that you send to be saved in your mailbox's *Sent* folder. Individual users can modify this setting from the Options→Compose page within WorldClient.

Display time using AM/PM

Click this option if you want a 12-hour clock with AM/PM to be used when times are displayed for this domain within WorldClient. Clear the check box if you want to use a 24-hour clock for the domain. Individual users can modify this setting from the Options→Calendar page within WorldClient.

Compose in new browser window

Click this option if you want a separate browser window to open for composing messages instead of simply switching the main window to the compose screen. Clear the box if you do not want separate windows to open. Individual users can modify this setting from the Options→Compose page within WorldClient.

Empty trash on exit

This option causes the user's trash to be emptied when he or she signs out from WorldClient. Individual users can modify this setting from the Options→Personalize page within WorldClient.

Use advanced compose

Click this option to cause the Advanced Compose rather than the normal Compose screen to be opened by default for the domain's users. Individual users can modify this setting from the Options→Compose page within WorldClient.

Enable ComAgent support

This option makes the ComAgent messaging utility available to the selected domain's users. They can download it from the Options→ComAgent page within WorldClient. The downloaded installation file will be automatically customized for each user's account to make installation and setup easier.

Enable Instant Messaging (MDaemon PRO only)

Click this option if you want to activate ComAgent's instant messaging (IM) system for the selected domain's users. Clear the check box if you want the instant messaging controls to be unavailable.

Log all IM traffic at the server level (MDaemon PRO only)

Click this check box if you want all of the selected domain's instant messaging traffic to be included in the `InstantMessaging.log` file (located in the `MDaemon/LOGS/` folder).

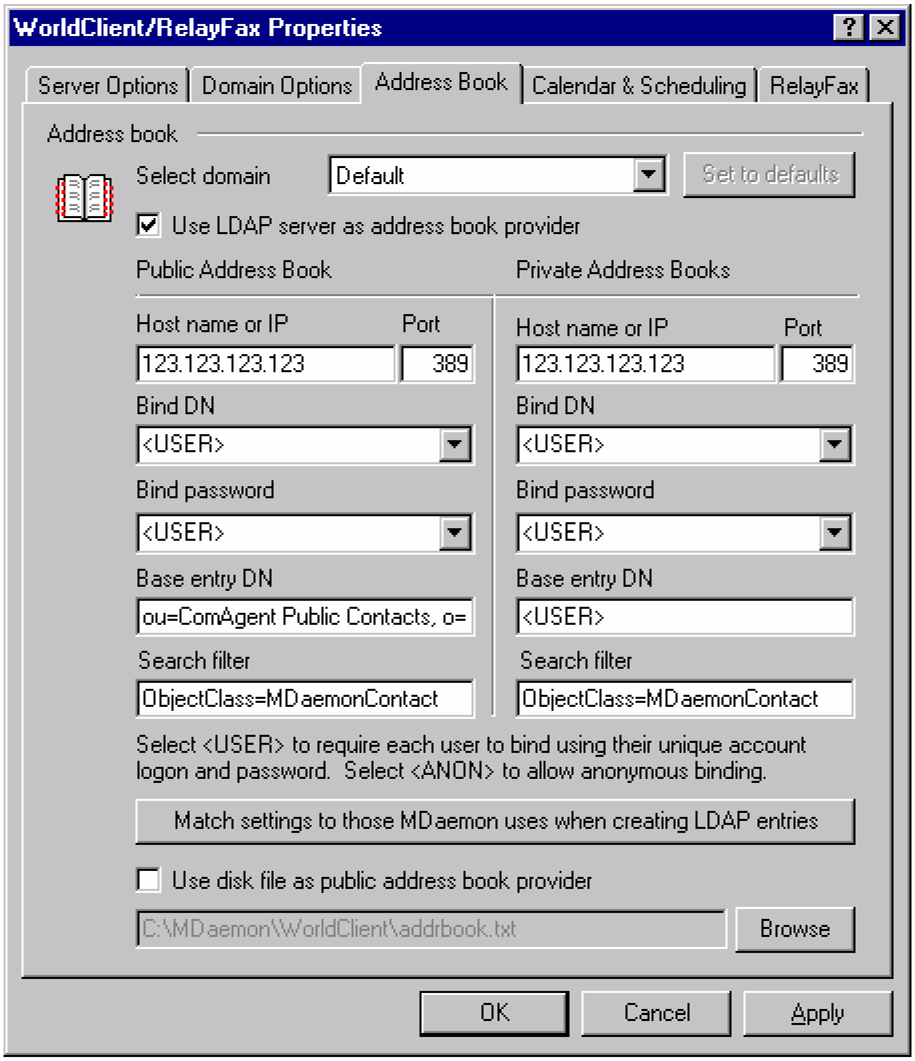
IM buddy list includes members of other domains

Click this option if you want all of your MDaemon domains' users to be available for adding to the selected domain's buddy lists. Clear this checkbox if you want only users of the same domain to be available for adding to buddy lists. For example, if your MDaemon is hosting mail for example.com and mycompany.com then activating this control for your example.com users will enable them to add buddies to their lists from both domains. Clearing it would mean that they could only add other example.com users.

Reminders sent via IM system are sent 'From:'

When an Appointment or Meeting is scheduled on a user's WorldClient calendar, the event can be set to send a reminder to the user at a specified time. If the IM system is active for the user's domain then the reminder will be sent in an instant message if he or she is using ComAgent. Use this text box to specify the name that you wish the message to appear to be 'From:'

Address Book



Address book

Select domain: Default

☑ Use LDAP server as address book provider

	Public Address Book	Private Address Books
Host name or IP	123.123.123.123	123.123.123.123
Port	389	389
Bind DN	<USER>	<USER>
Bind password	<USER>	<USER>
Base entry DN	ou=ComAgent Public Contacts, o=	<USER>
Search filter	ObjectClass=MDaemonContact	ObjectClass=MDaemonContact

Select <USER> to require each user to bind using their unique account logon and password. Select <ANON> to allow anonymous binding.

☐ Use disk file as public address book provider

C:\MDaemon\WorldClient\addrbook.txt

Address Book

Select domain

Use this drop-down list to choose the domain whose address book settings you wish to edit. Leave it set to *Default* if you wish to edit the default settings. The default settings will be used for all domains whose settings you haven't specifically changed. If you make changes to any of the settings on this tab then you must *Apply* them before switching to a different *Select domain* setting. If you make changes and then attempt to select a different domain without first applying them, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

Set to defaults

This option resets a domain to the *Default* address book settings. Use the *Select domain* control to select a domain and then click *Set to defaults* to restore it.

Use LDAP server as address book provider

Click this option if you want to use an LDAP server as WorldClient's Public and Private address book provider. If you clear this option then a local, plain text disk file will be used for the address book (see *Use disk file as public address book provider* below). When using an LDAP server as your address book provider, each contact contains a number of fields that may be edited from within WorldClient. See *Automatic Address Book Synchronization* (page 87) for the complete list of the Address Book contact fields.

Public and Private Address Book Settings

The following six options (*Host name or IP* through *Search filter*) are listed in two identical columns on the Address Book tab. Although the controls in both columns have identical functions, the first column applies to the Public Address Book and the second column applies to the Private.

Host name or IP

Enter the host name or IP address of the LDAP server that you want to use as the address book provider.

Port

This is the port on which the LDAP server will listen for connections from WorldClient.

Bind DN

This is the distinguished name (DN) that will be used in the bind operation for authentication. In most cases you should leave this control set to <USER>, which will require each user's unique logon credential rather than a single global value. Choosing <ANON> will allow anonymous binding rather than require authentication.

Bind password

This is the password value used in the bind operation. In most cases you should leave this set to <USER> (see Bind DN above) so that each user's unique password will be required.

Base entry DN

Enter the base entry (root DN) that will be used for the address book. For the Public Address Book, this should be a static rather than dynamic value so that all users will see the same public addresses. If you are using the LDAP Options tab (page 94) to mirror your MDaemon accounts to an LDAP address book, the Public *Base entry DN* will usually be the same as the *Base entry DN (address book)* value on that tab. The Private Address Book's *Base entry DN* should normally be set to <USER>. This will cause it to have a dynamic value so that each user can have an individual private address book that only he or she can access. If you set the Private *Base entry DN* to a static value then that will effectively cause all users to share a single private address book.

Search filter

The value of this option should normally be set to the ObjectClass of the entries that you want to be searched when using the Search feature in WorldClient's Address Book. The *Search filter's* default setting is `ObjectClass=MDaemonContact`.

Match settings to those MDaemon uses when creating LDAP entries

Click this button to change the *Bind DN* and *Bind password* values of the Public and Private address books to their corresponding values on the LDAP Options tab (see page 94). Normally you should leave those options set to <USER> to require each user to bind using their unique account credentials.

Note

If you are not using LDAP Options to mirror your MDaemon account database to an LDAP server then this control will be unavailable.

Use disk file as public address book provider

If you wish to use a plain text file as WorldClient's Public Address book rather than an LDAP database, click this option and specify the location of the file. When this option is selected, each user's Private Address Book will also be maintained in a plain text file called `addrbook.txt`. The Private Address Book file is located in each user's `WC` subfolder (for example `\USERS\example.com\HFord\WC`). This subfolder and file will be created the first time a user creates a private contact from within WorldClient. Address Book text files are tab delimited, and each entry may contain a name, email address, and comment in that order.

Automatic Address Book Synchronization

By using ComAgent in conjunction with Alt-N's LDaemon LDAP server (v2.0 or later) to maintain WorldClient's Public and Private address books, you can provide two-way synchronization between LDaemon and the Outlook/Outlook Express address book on each user's local computer. Thus, if you use both Outlook or Outlook Express and WorldClient at different times, the address books will match in both products.

MDaemon can maintain an accurate and continuously up to date LDAP database of users by communicating with LDaemon each time an MDaemon account is added, removed, or modified (see *LDAP Options*—Page 94 for more information). ComAgent has the ability to poll LDaemon at regular intervals and acquire all the contact information being stored there. It then publishes this information to the local computer's Windows Address Book or contact store. This has the effect of instantaneously updating any local software package which uses the local address book system (for example, Outlook/Outlook Express).

Anyone using ComAgent with the proper LDaemon access credentials can also add Public contacts by using the Windows Address Book directly, or through Outlook/Outlook Express. The new contact will be picked up by ComAgent and uploaded to LDaemon. From there all other users on your network will have access to the new contact the next time their ComAgent poles LDaemon.

You must create two folders within your Windows Address Book to store contact information: "ComAgent Public Contacts" contains contacts that you wish to share with all ComAgent users on your network. "ComAgent Private Contacts" are personal contacts that may be seen only by you. Optionally, you can change these default folder values via settings on the Address Book tab of ComAgent Properties.

Note

Windows Address Book (WAB) synchronization requires IE 5 or greater with identity support enabled.

The following address book fields will be synchronized:

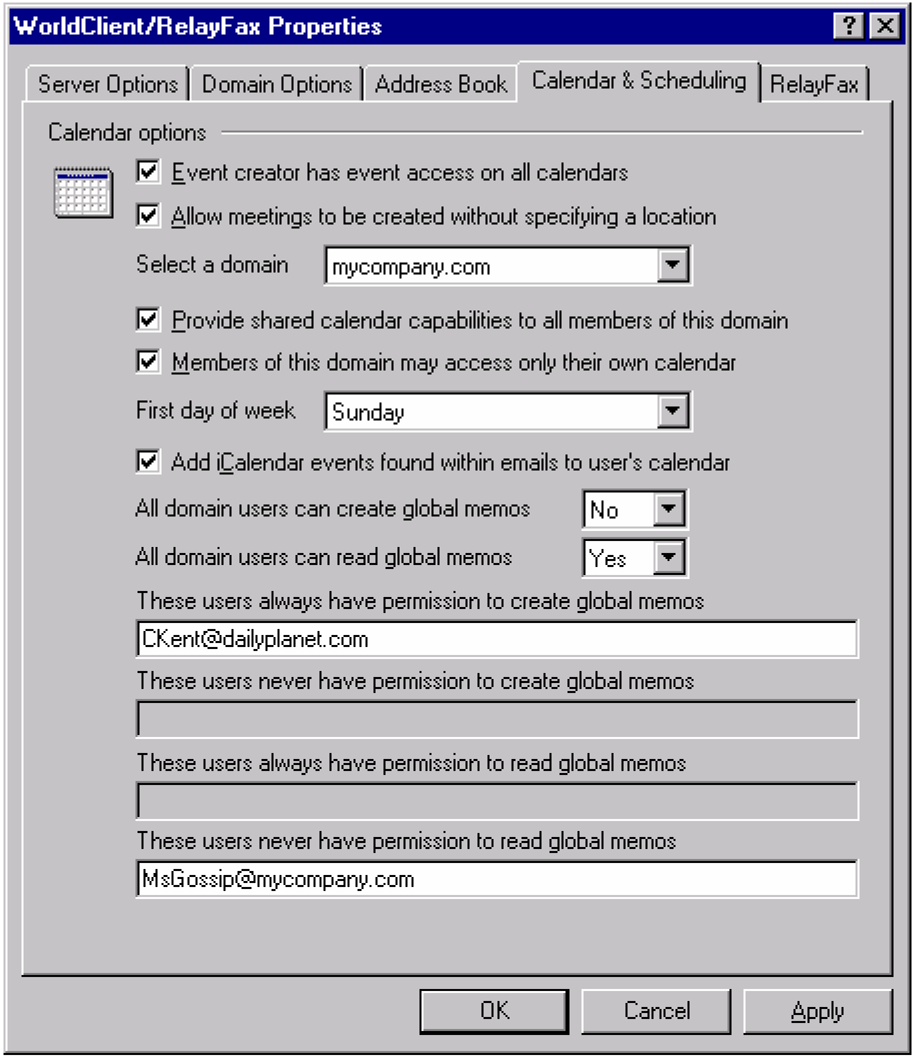
Full name
Home Address
Home City
Home State
Home Zip
Home Country
Home Phone
Home Fax
Home Mobile
Home Web Address
Business Company
Business Address
Business City
Business State
Business Zip
Business Country
Business Title
Business Department
Business Office
Business Phone
Business Fax
Business Pager
Business IP Phone
Business Web Address
Comments

For more information on the various Address Book options within MDaemon and WorldClient see:

LDAP Options—Page 94

Miscellaneous Options | *WAB*—Page 209

Calendar & Scheduling



Calendar options

☑ Event creator has event access on all calendars

☑ Allow meetings to be created without specifying a location

Select a domain: mycompany.com

☑ Provide shared calendar capabilities to all members of this domain

☑ Members of this domain may access only their own calendar

First day of week: Sunday

☑ Add iCalendar events found within emails to user's calendar

All domain users can create global memos: No

All domain users can read global memos: Yes

These users always have permission to create global memos: CKent@dailyplanet.com

These users never have permission to create global memos:

These users always have permission to read global memos:

These users never have permission to read global memos: MsGossip@mycompany.com

Calendar Options

Event creator has event access on all calendars

This is a global setting; it cannot be set per domain.

Allow meetings to be created without specifying a location

Click this option if you do not want to require that users specify a meeting location whenever a meeting event is created. Clear the check box if you want to force all meetings to have a location specified when they are scheduled. This is a global setting; it cannot be set per domain.

Select a domain

Use this drop-down list to choose the domain whose Group Scheduling and Calendar settings you wish to edit. If you make changes to any of the settings on this tab then you must *Apply* them before switching to a different *Select domain* setting. If you make changes and then attempt to select a different domain without first applying them, a box will appear asking you to choose whether or not you wish to save the changes before switching to the new domain. Click *Yes* to save the changes or *No* to discard them.

Provide shared calendar capabilities to all members of this domain

Click this option if you want to make the Calendar System available to WorldClient users of the selected domain. If you clear this option the Calendar System will be disabled for the domain, and there will be no calendar link on WorldClient's navigation bar.

Members of this domain may access only their own calendar

Click this option if you wish to prevent the domain's users from being able to view each other's calendar.

First day of week

Choose a day from the drop-down list. The selected day will appear in the domain's calendars as the first day of the week.

Add iCalendar events found within emails to user's calendar

WorldClient supports Internet Calendaring (iCal) used in Microsoft Outlook and other iCal compliant email programs. Click this option if you want iCalendar events that WorldClient finds within email messages addressed to a WorldClient user to be added automatically to his or her calendar.

All domain users can read global memos

Set this drop-down box to "Yes" if you want global memos to appear on every WorldClient user's calendar. Set it to "No" if you don't. You can designate specific users as exceptions to this setting by using the text boxes below labeled, "*These users always/never have permission to read global memos*." These controls are set per domain.

All domain users can create global memos

Set this drop-down box to "Yes" if you want to give all of the selected domain's WorldClient users permission to create global memos. Set it to "No" if you don't. You can designate specific users as exceptions to this setting by using the text boxes below labeled, "*These users always/never have permission to create global memos*."

These users always have permission to create global memos

Use this control to enter the email addresses of WorldClient users whom you wish to be treated as exceptions when "*All domain users can create global memos*" is set to "No". The specified users **will** be able to create global memos. Separate multiple addresses by commas.

These users never have permission to create global memos

Use this control to enter the email addresses of WorldClient users whom you wish to be treated as exceptions when "*All domain users can create global memos*" is set to "Yes". The specified users **will not** be able to create global memos. Separate multiple addresses by commas.

These users always have permission to read global memos

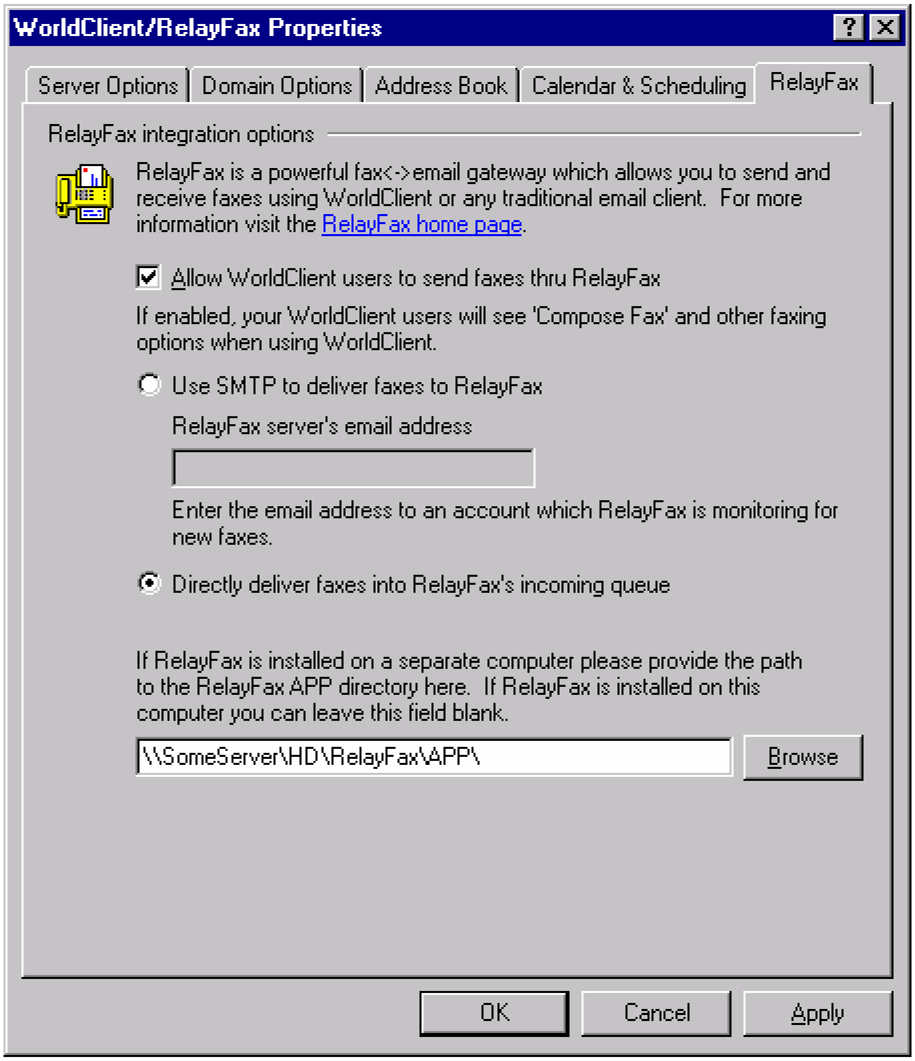
Use this control to enter the email addresses of WorldClient users whom you wish to be treated as exceptions when "*All domain users can read global memos*" is set to "No". The specified users **will** be able to read global memos. Separate multiple addresses by commas.

These users never have permission to read global memos

Use this control to enter the email addresses of WorldClient users whom you wish to be treated as exceptions when "*All domain users can read global memos*" is set to "Yes". The specified users **will not** be able to read global memos. Separate multiple addresses by commas.

RelayFax Integration

Alt-N Technologies' RelayFax Server is an email to fax and fax to email gateway that can be integrated seamlessly with WorldClient in order to provide fax services to your users. When this functionality is enabled, WorldClient users will be given access to various features that will enable them to compose and send faxes via the WorldClient client pages. For more information about RelayFax, visit the RelayFax web site at www.relayfax.com.



RelayFax integration options

RelayFax is a powerful fax<->email gateway which allows you to send and receive faxes using WorldClient or any traditional email client. For more information visit the RelayFax home page.

☑ Allow WorldClient users to send faxes thru RelayFax

If enabled, your WorldClient users will see 'Compose Fax' and other faxing options when using WorldClient.

○ Use SMTP to deliver faxes to RelayFax

RelayFax server's email address

Enter the email address to an account which RelayFax is monitoring for new faxes.

● Directly deliver faxes into RelayFax's incoming queue

If RelayFax is installed on a separate computer please provide the path to the RelayFax APP directory here. If RelayFax is installed on this computer you can leave this field blank.

\\SomeServer\HD\RelayFax\APP\

RelayFax Integration Options

Allow WorldClient users to send faxes thru RelayFax

Click this option to integrate RelayFax with WorldClient. When active it will cause a "Compose Fax" control and other fax related features to appear on the WorldClient pages.

Use SMTP to deliver faxes to RelayFax

RelayFax monitors a specific mailbox for incoming messages that are to be faxed. Click this option and MDaemon will use the normal SMTP email delivery process to send these messages to that mailbox's address. This option is useful when RelayFax is monitoring a mailbox located somewhere other than your LAN. If RelayFax resides on your LAN you may choose to have MDaemon deliver the messages directly to RelayFax's message queue and thus bypass the SMTP delivery process altogether. For more information on this method, see *Directly deliver faxes into RelayFax's incoming queue* below.

RelayFax server's email address

Specify the email address to which you want messages intended for faxing to be delivered. This value must match the address that you have configured RelayFax to monitor for these messages.

Directly deliver faxes into RelayFax's incoming queue

If RelayFax resides on your LAN you may choose this method rather than SMTP for distributing messages to it for faxing. When MDaemon receives a message intended for RelayFax it will place it directly into RelayFax's incoming queue rather than deliver it using SMTP. If RelayFax resides on the same machine on which MDaemon is running you may leave the file path field blank. Otherwise, you must specify the network path to RelayFax's `\app\` directory.

Chapter

7

LDaemon/Address Book Options

Using LDAP and Supporting Global Address Books.

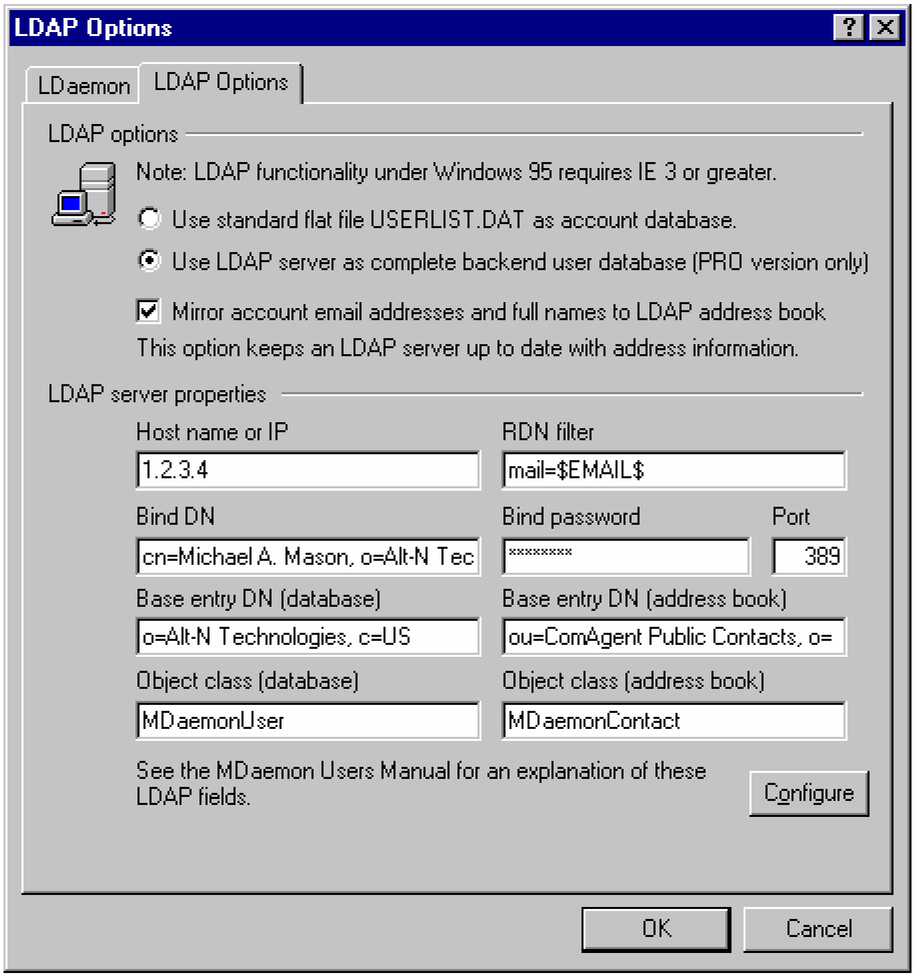
MDaemon version 6 supports Lightweight Directory Access Protocol (LDAP) functionality. Click **Setup| LDaemon/Address book options…** to open the LDAP Options dialog used for configuring MDaemon to keep your LDAP server up to date on all of its user accounts. This makes it possible for users with mail clients that support LDAP to "share" a global address book that will contain entries for all of your MDaemon users as well as any other contacts that you include.

You can use your LDAP server as the MDaemon user database rather than its local `USERLIST.DAT` system. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

You can also use this dialog for managing Alt-N's LDaemon LDAP server. You can obtain this standards-based LDAPv3 server free of charge from www.altn.com.

For information on using an LDAP server as the Public and Private address book provider for your WorldClient users, see the **Address Book** tab of the **WorldClient/RelayFax Properties** dialog—page 85.

LDAP Options



LDAP options

Note: LDAP functionality under Windows 95 requires IE 3 or greater.

○ Use standard flat file USERLIST.DAT as account database.

● Use LDAP server as complete backend user database (PRO version only)

☑ Mirror account email addresses and full names to LDAP address book

This option keeps an LDAP server up to date with address information.

LDAP server properties

Host name or IP: 1.2.3.4

RDN filter: mail=$EMAIL$

Bind DN: cn=Michael A. Mason, o=Alt-N Tec

Bind password: ********

Port: 389

Base entry DN (database): o=Alt-N Technologies, c=US

Base entry DN (address book): ou=ComAgent Public Contacts, o=

Object class (database): MDaemonUser

Object class (address book): MDaemonContact

See the MDaemon Users Manual for an explanation of these LDAP fields.

LDAP Options

Use standard flat file USERLIST.DAT as account database

Choose this option if you want MDaemon to use its internal `USERLIST.DAT` file as the account database. This is MDaemon's default setting and causes all of the MDaemon user account information to be stored locally.

Use LDAP server as complete backend user database (PRO version only)

Select this option if you want MDaemon to use your LDAP server as the MDaemon user database rather than its local `USERLIST.DAT` system. You might want to use this method of maintaining your user information if you have multiple MDaemon servers at different locations but want them to share a single user database. Each MDaemon server would be configured to connect to the same LDAP server in order to share user information rather than storing it locally.

Mirror account email addresses and full names to LDAP address book

If you are using the default `USERLIST.DAT` method of maintaining your account database rather than the LDAP server method, you can still keep an LDAP server up to date on all of your users' names and email addresses by enabling this checkbox. Thus, you can use the LDAP server as a global address book system for your users without having to use it as a complete backend user database.

LDAP Server Properties

Host name or IP
Enter the host name or IP address of your LDAP server here.

RDN filter
This control is used to generate the RDN for each user's LDAP entry. The relative distinguished name (RDN) is the leftmost component in each entry's distinguished name (DN). For all peer entries (those sharing a common immediate parent) the RDN must be unique, therefore we suggest using each user's email address as their RDN to avoid possible conflicts. Using the $EMAIL$ macro as the value of the attribute in this control (i.e. `mail=$EMAIL$`) will cause it to be replaced by the user's email address when their LDAP entry is created. The user's DN will be comprised of the RDN plus the *Base entry DN* below.

Bind DN
Enter the DN of the entry to which you have granted administrative access to your LDAP server so that MDaemon can add and modify your MDaemon user entries. This is the DN used for authentication in the bind operation.

Bind Password
This password will be passed to your LDAP server along with the *Bind DN* value for authentication.

Port
Specify the port that your LDAP server is monitoring. MDaemon will use this port when posting account information to it.

Base entry DN (database)
Enter the base entry (root DN) that will be used in all of your MDaemon user entries when you are using the LDAP server as your user database rather than the `USERLIST.DAT` file. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Base entry DN (address book)
When mirroring account information to an LDAP database address book, enter the base entry (root DN) that will be used in all of your MDaemon user address book entries. The Base entry DN is combined with the RDN (see *RDN filter* above) to make up each user's distinguished name (DN).

Object class (database)
Specify the object class to which each MDaemon user's user database entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

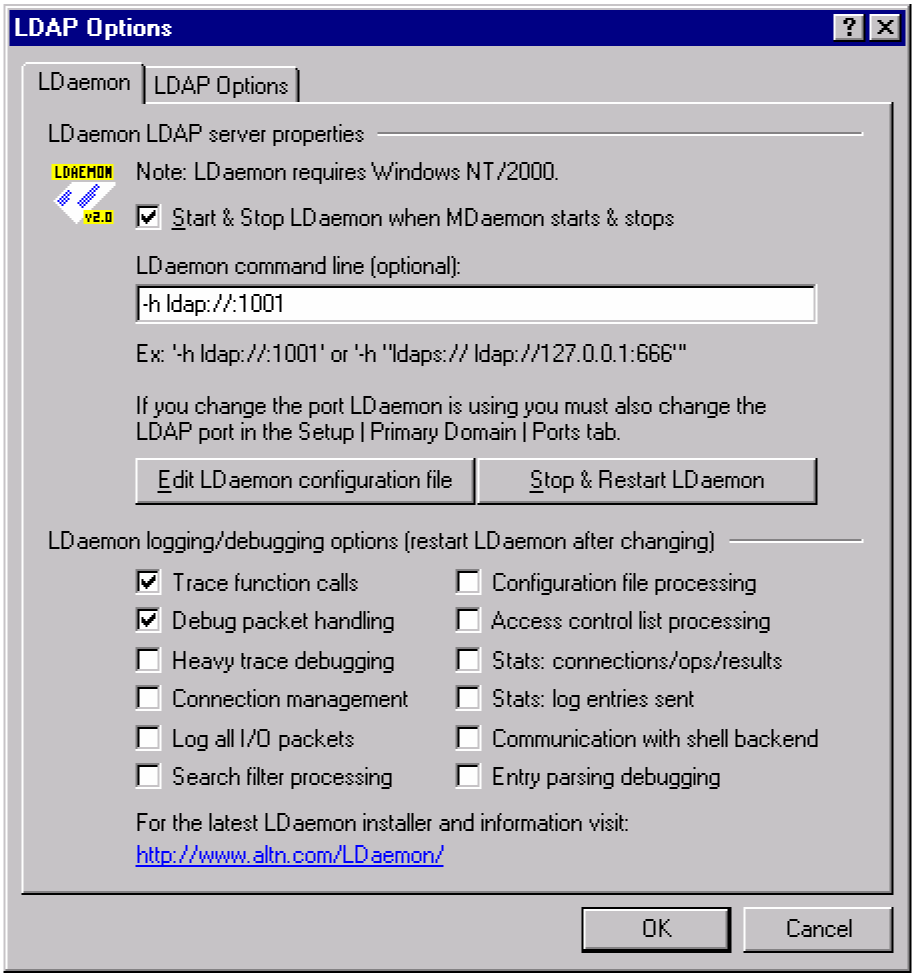
Object class (address book)
Specify the object class to which each MDaemon user's LDAP address book entry must belong. Each entry will contain the `objectclass=` attribute with this as its value.

Configure

Click this button to open the `LDAP.dat` configuration file in a text editor. It is used for designating the LDAP attribute names that will correspond to each MDaemon account field.

For information on using an LDAP server as the Public and Private address book provider for your WorldClient users, see the Address Book tab of the WorldClient/RelayFax Properties dialog—page 85.

LDaemon LDAP Server



LDaemon LDAP server properties

Note: LDaemon requires Windows NT/2000.

☑ Start & Stop LDaemon when MDaemon starts & stops

LDaemon command line (optional):

```
-h ldap://:1001
```

Ex: '-h ldap://:1001' or '-h "ldaps:// ldap://127.0.0.1:666"'

If you change the port LDaemon is using you must also change the LDAP port in the Setup | Primary Domain | Ports tab.

LDaemon logging/debugging options (restart LDaemon after changing)

☑ Trace function calls
☑ Debug packet handling
☐ Heavy trace debugging
☐ Connection management
☐ Log all I/O packets
☐ Search filter processing
☐ Configuration file processing
☐ Access control list processing
☐ Stats: connections/ops/results
☐ Stats: log entries sent
☐ Communication with shell backend
☐ Entry parsing debugging

For the latest LDaemon installer and information visit:
http://www.altn.com/LDaemon/

This tab is used to control Alt-N Technologies' LDaemon LDAP server. Note: these controls will not be available until LDaemon has been installed. LDaemon can be downloaded free of charge from `ftp://ftp.altn.com/LDaemon/`.

LDaemon LDAP Server Properties

Start & Stop LDaemon when MDaemon starts & stops
Click this checkbox if you want to launch the LDaemon LDAP server when MDaemon starts, and stop it when MDaemon stops.

LDaemon command line (optional)
If you wish to utilize some command line switches for LDaemon you can do so by typing the command line into this control.

Edit LDaemon configuration file
Click this button to open the LDaemon configuration file for editing in the default text editor.

Stop & Restart LDaemon

After make any changes to LDaemon, click this button to stop and restart the LDAP server so that your changes will be implemented.

LDaemon Logging/Debugging Options

This section contains various logging/debugging options for LDaemon. You must restart LDaemon after making any changes to these options before the new settings will take effect.

Chapter

8

Shared Folders/Mail Queues

Creating additional mail queues, and configuring and utilizing Shared IMAP folders.

MDaemon version 6 supports Shared IMAP Folders—Public and User folders may both be shared. Public folders are extra folders that do not belong to any particular account but can be made available to multiple IMAP users. User folders are IMAP folders that belong to individual MDaemon accounts. Not to be confused with public FTP or html folders, MDaemon's Shared IMAP folders, whether Public or User, may not be accessed by everyone. Each shared folder must have a list of MDaemon users associated with it, and only members of that access list may access it via WorldClient or an IMAP email client.

When IMAP users access their list of personal folders, shared public folders and shared user folders to which they have been given access will also be displayed. In this way certain mail folders can be shared by multiple users but still require each user's individual logon credentials. Further, having access to a folder doesn't necessarily mean having full read/write or administrative access to it. Specific access rights can be granted to individual users, thus allowing you to set different levels of access for each one. For example, you might allow some users to delete messages while restricting that from others.

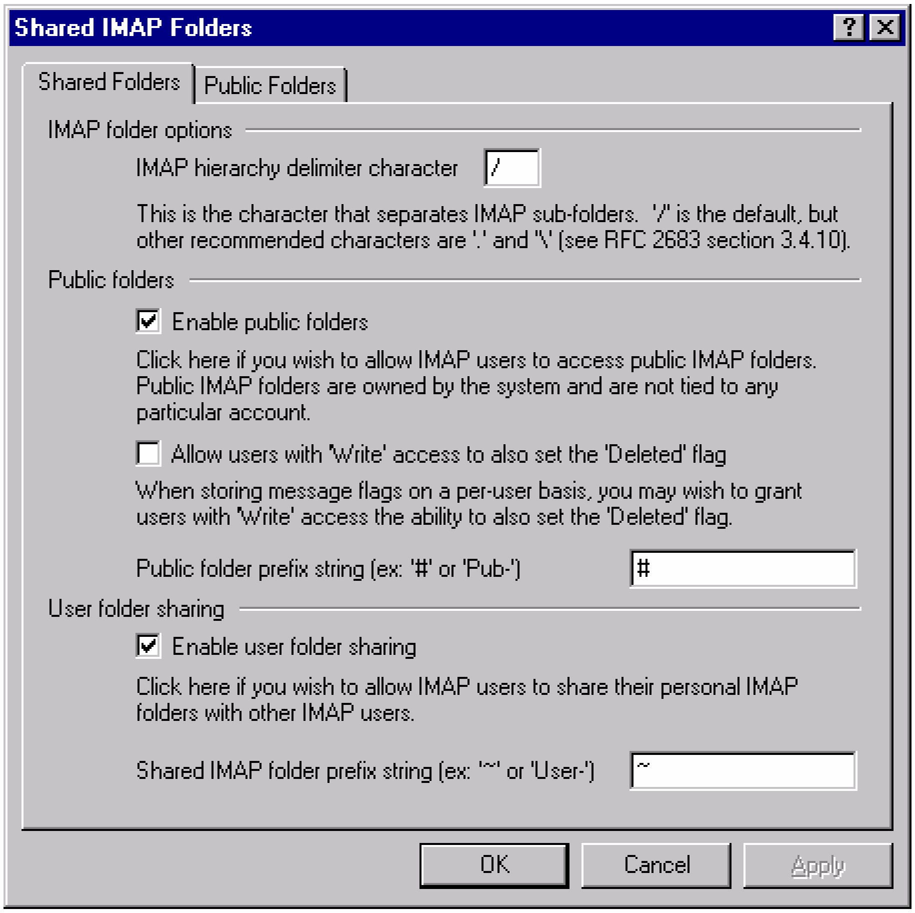
Once a public or user IMAP folder has been created you can use the Content Filter to set criteria by which certain messages are moved into that folder. For example, it might be useful to make a rule that would cause messages containing `support@mydomain.com` in the `TO:` header to be moved into the `Support` public folder. The Content Filter actions "`Move Message to Public Folders`…" and "`Copy Message to Folder`…" make this possible. For shared user folders, you can use your personal IMAP Mail Rules to route specific messages to them. In addition to using Content Filters and IMAP Mail Rules, you can associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

For added convenience, the mailing list editor also contains a Public Folders tab that makes it possible for you to configure a public folder for use with a particular list. If you enable this feature then a copy of each list message will be placed into the specified public folder. All public folders are stored in the `\Public Folders\` directory within the MDaemon directory hierarchy.

Shared IMAP Folders

To reach the Shared IMAP Folders dialog click Setup→Shared IMAP Folders… on MDaemon's menu bar.

Shared Folders



IMAP folder options

IMAP hierarchy delimiter character: /

This is the character that separates IMAP sub-folders. '/' is the default, but other recommended characters are '.' and '\' (see RFC 2683 section 3.4.10).

Public folders

☑ Enable public folders

Click here if you wish to allow IMAP users to access public IMAP folders. Public IMAP folders are owned by the system and are not tied to any particular account.

☐ Allow users with 'Write' access to also set the 'Deleted' flag

When storing message flags on a per-user basis, you may wish to grant users with 'Write' access the ability to also set the 'Deleted' flag.

Public folder prefix string (ex: '#' or 'Pub-'): #

User folder sharing

☑ Enable user folder sharing

Click here if you wish to allow IMAP users to share their personal IMAP folders with other IMAP users.

Shared IMAP folder prefix string (ex: '~' or 'User-'): ~

IMAP Folder Options

IMAP hierarchy delimiter character

Type the character that you want to denote a subfolder when used in a folder name. For example, if this character is set to "/" and you have a folder on the Public Folders tab called "My Folder", then to create a subfolder under it you would name your new folder "My Folder/My Subfolder". Whenever IMAP users connect to MDaemon, "My Subfolder" will be listed in their folders as a subfolder of "My Folder".

Note: Although a subfolder will be displayed as a subfolder in your list of IMAP folders in your email client, it is not actually a subfolder on the server. It is a parent folder containing the folder and subfolder names separated by the delimiter character.

Public Folders

Enable public folders

Click this switch if you wish to allow IMAP users to gain access to public folders. The users that can access them and the level of access granted is designated under each folder on the Public Folders tab. Clear this check box if you want to hide public folders from all users.

Allow users with 'Write' access to also set the 'Deleted' flag

'Write' access means users can 'flag' messages as read, unread, and so on. Click this check box if you want users to whom you have granted 'write' access permission to be able be to flag messages as 'deleted' as well.

Public folder prefix string (ex: '#' or 'pub-')

Public folders are prefixed with a sequence of up to 20 characters, such as '#' or 'Public-'. This is to help users easily distinguish public from private folders from within their email client software. Use this text box to specify the series of characters that you wish to use to denote public folders.

User Folders Sharing

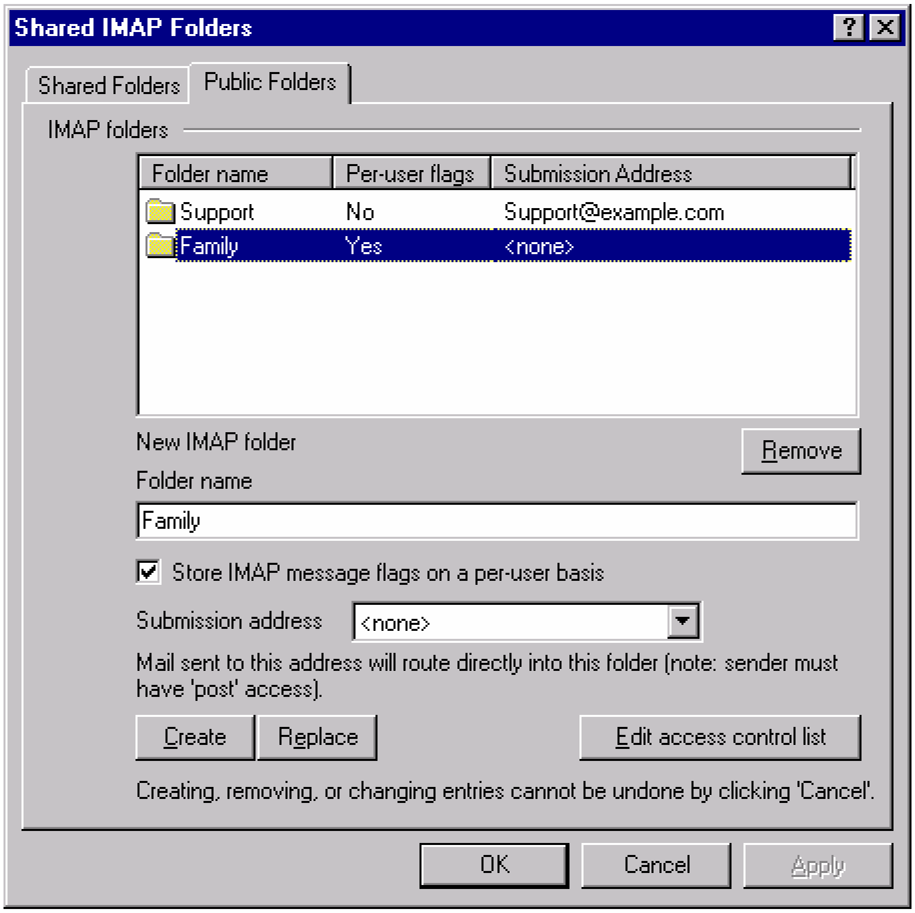
Enable user folder sharing

Click this switch if you wish to allow IMAP users to share access to their IMAP folders. The users that can access them and the level of access granted is designated under each folder on the Shared Folders tab of the Account Editor (Accounts→Account Manager…→User Account on MDaemon's menu bar). Clear this check box if you want to prevent users from being able to share access to their folders.

Shared IMAP folder prefix string (ex: '-' or 'User-')

Shared user folders are prefixed with a sequence of up to 20 characters, such as '-' or 'User-'. This is to help users easily distinguish shared from private folders from within their email client software. Use this text box to specify the series of characters that you wish to use to denote shared user folders.

Public Folders



IMAP folders

Folder name	Per-user flags	Submission Address
Support	No	Support@example.com
Family	Yes	<none>

New IMAP folder

Folder name: Family

☑ Store IMAP message flags on a per-user basis

Submission address: <none>

Mail sent to this address will route directly into this folder (note: sender must have 'post' access).

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

IMAP Folders

Displayed in this area is each public IMAP folder that you have created, the *Per-user flags* setting, and the Submission Address with which each one has been associated (if any). When MDaemon is first installed, this area will be empty until you use the *Folder name* and *Create* controls to add a folder to it. Subfolders in this list will have the folder and subfolder names separated by the delimiter character designated on the Shared Folders tab.

Remove

To remove a public IMAP folder from the list, select the desired folder and then click the Remove button.

New IMAP Folder

Folder name

To add a new folder to the list, specify a name for it in this control, set the per-user flags and Submission address controls, and then click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, then prefix the new folder's name with the parent folder's name and the delimiter character designated on the Shared Folders tab. For example, if the delimiter character is '/' and parent folder is "My Folder" then the new subfolder name would be "My Folder/My New Folder". If you don't want it to be a subfolder, then name the new folder "My New Folder" without the prefix.

Store IMAP message flags on per-user basis

Click this check box if you want the folder's message flags (read, unread, replied to, forwarded, and so on) to be set on a per-user basis instead of globally. Each user will see the status of the messages in the shared folder displayed according to their personal interaction with them. A user who hasn't read a message will see it flagged as 'unread' while a user who has read it will see the status as 'read'.

If this control is disabled then all users will see the same status. So, once any user has read a message then all users will see it marked as 'read'.

Submission address

Use this drop-down list to associate a specific account with a shared folder so that messages destined for that "Submission Address" will be automatically routed to the shared folder. However, only users who have been granted "post" permission to the folder will be able to send to that address.

Create

After specifying a folder's name and other settings, click this button to add the folder to the list.

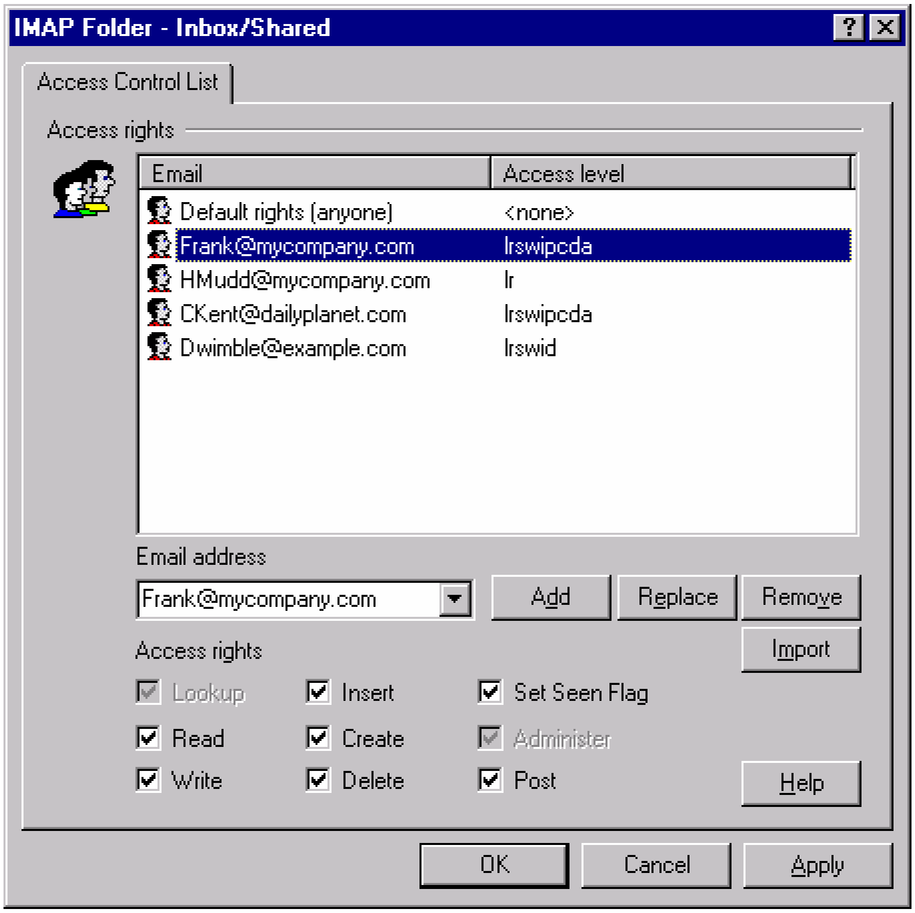
Replace

If you wish to edit one of the Public Folders entries, click the entry, make the desired changes to the *Folder name* or other setting, and then click the *Replace.*

Edit access control list

Choose a folder and then click this button to open the Access Control List dialog for that folder. Use the Access Control List dialog to designate the users that will be able to access the folder and the permissions for each user.

Access Control List



Email	Access level
Default rights (anyone)	<none>
Frank@mycompany.com	lrswipcda
HMudd@mycompany.com	lr
CKent@dailyplanet.com	lrswipcda
Dwimble@example.com	lrswid

Email address: Frank@mycompany.com

Access rights

☑ Lookup ☑ Insert ☑ Set Seen Flag

☑ Read ☑ Create ☑ Administer

☑ Write ☑ Delete ☑ Post

Access Rights

This area is for designating the MDaemon user accounts that you wish to grant access to the shared folder, and for setting the access permissions for each one. You can reach this dialog from the Public Folders tab of the Shared IMAP Folders dialog (click Setup→Shared IMAP Folders...→Public Folders). Double-click the desired folder, or click the folder and then click *Edit access control list*, to open the Access Control dialog for that folder. Each entry lists the email address of the account and a one letter Access Level abbreviation for each Access Right that you grant to the user.

Email address

From the drop-down list, choose the MDaemon account that you wish to grant access to the shared folder.

Add

After choosing an Email Address from the list, and the access rights that you wish to grant to the user, click *Add* to add the account to the list.

Replace

To modify an existing Access Rights entry, select the entry, make any desired changes to the Access Rights, and then click *Replace*.

Remove

To remove an entry from the Access Rights list, select the desired entry and then click *Remove*.

Import

With the *Import* feature you can add the members of an existing Mailing List to the list of users with Access Rights. Choose the access rights that you wish to grant to the users, click Import, and then double-click the desired list. All of the list's members will be added to the list with the rights that you set.

Access Rights

Choose the rights that you wish to grant to individual users by clicking the desired options in this area and then clicking *Add* for new entries or *Replace* for existing entries.

You can grant the following Access Control Rights:

Lookup (l) – user can see this folder in their personal list of IMAP folders.
Read (r) – user can open this folder and view its contents.
Write (w) – user can change flags on messages in this folder.
Insert (i) – user can append and copy messages into this folder.
Create (c) – user can create subfolders within this folder.
Delete (d) – user can delete messages from this folder.
Set Seen Flag (s) – user can change the read/unread status of messages in this folder.
Administer (a) – user can administer the ACL for this folder.
Post (p) – user can send mail directly to this folder (if folder allows).

Help

Click *Help* to display a list of the access rights and their definitions.

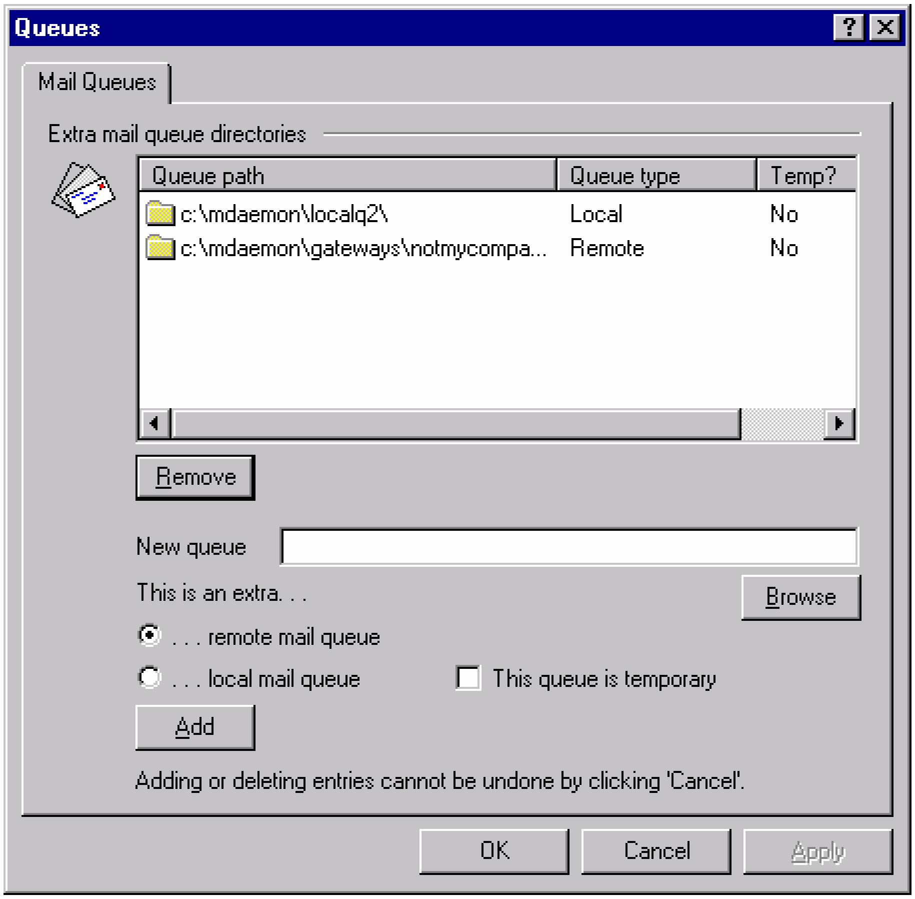
Note

Access rights are controlled through support for Access Control Lists (ACL) that has been added to MDaemon 6.0. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access rights to your folders to other users who also have accounts on your mail server. If your email client doesn't support ACL you can still set the permissions via the controls on this dialog. Currently very few email clients support ACL directly but there is an excellent utility from www.bynari.net called InsightConnector that will add this functionality (and more) to Microsoft Outlook.

ACL is fully discussed in RFC 2086, which can be viewed at:

`http://www.rfc-editor.org/rfc/rfc2086.txt`

Mail Queues



Extra mail queue directories

Queue path	Queue type	Temp?
c:\mdaemon\localq2\	Local	No
c:\mdaemon\gateways\notmycompa...	Remote	No

New queue

This is an extra. . .

● . . . remote mail queue

○ . . . local mail queue □ This queue is temporary

Adding or deleting entries cannot be undone by clicking 'Cancel'.

Use the Queues dialog (click Queues→Queues on the menu bar) to create custom local and remote mail queues. Custom queue support makes it possible for you to have MDaemon monitor several locations from which to send mail. On the Mail Queues tab you can create new queues, designating them as local or remote, and specify whether or not the new queue should be temporary. Temporary queues will be used at the next scheduled mail processing interval and then removed from the mail queue list. You can use Content Filters (page 166) to cause messages to be automatically placed into one of your custom mail queues.

Extra Mail Queue directories

This area displays an entry for each custom queue, lists whether it is local or remote, and whether it is temporary or permanent.

Remove

If you wish to remove a queue from the list, select its entry and then click the *Remove* button.

New queue

Use this text field to list the path to the folder that you wish to designate as a mail queue.

This is an Extra...

…remote mail queue
Choose this option if you want the custom mail queue to be used for remote mail.

…local mail queue
Choose this option if you want the custom mail queue to be used for local mail.

This queue is temporary
Click this checkbox if you want the queue to be temporary. It will be used during the next mail processing interval and then removed from the list.

Add
After you have listed the path to the new queue and designated its other parameters, click the *Add* button to add it to the list of custom queues.

Chapter

9

Security Settings

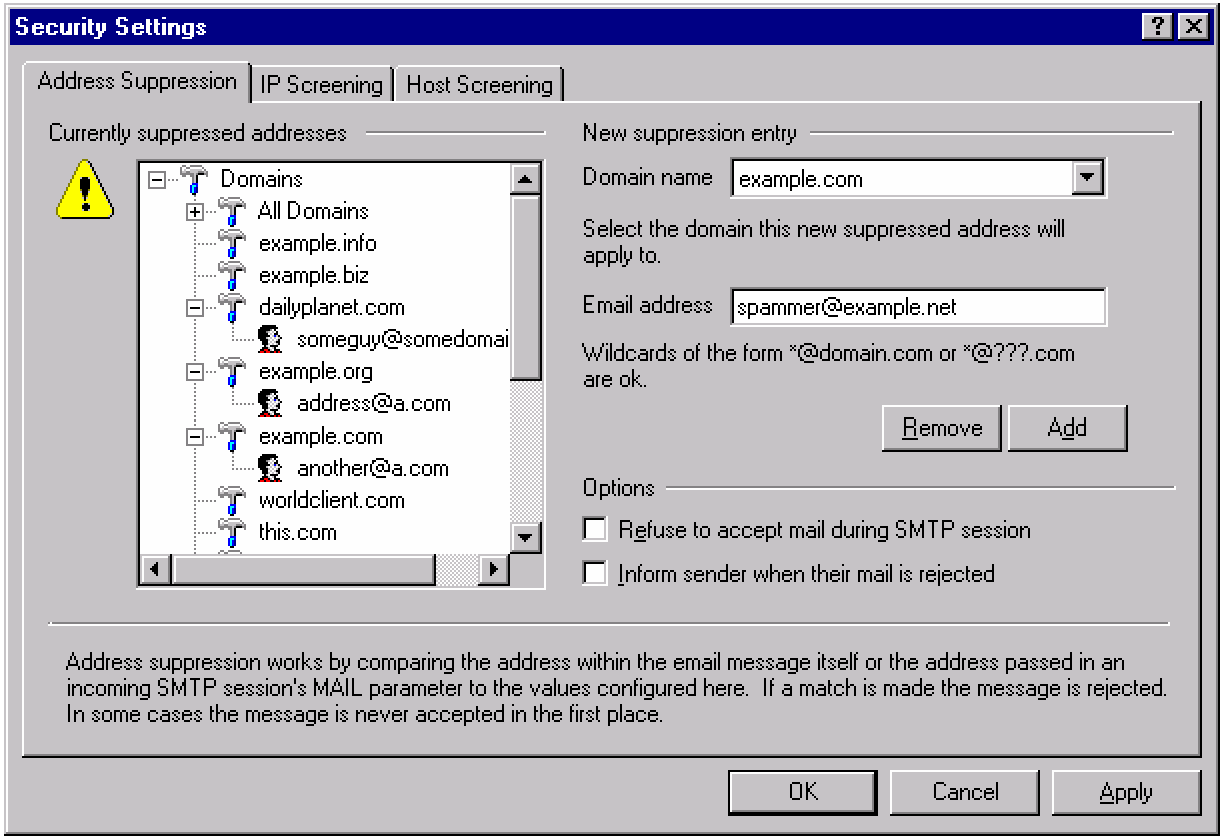
MDaemon's Security and Screening Features

MDaemon is equipped with an extensive suite of security features and controls. Click **Setup→Security Settings** on MDaemon's menu bar to reach the following security features:

Security Settings

- **Address Suppression**—Lists addresses that are not allowed to send mail traffic through your server.
- **IP Screening**—Used to designate IP addresses from which you will allow or refuse connections to your server.
- **Host Screening**—Used to designate hosts (domain names) from which you will allow or refuse connections to your server.
- **IP Shielding**—If a domain name specified in this list attempts to connect to your server, its IP address must match the one that you have assigned to it.
- **SMTP Authentication**—Used for setting several options that denote how MDaemon will behave when a user sending a message to MDaemon has or has not been authenticated first.
- **POP Before SMTP**—The controls on tab are used to require each user to first access his or her mailbox before being allowed to send a message through MDaemon, thus authenticating that the user is a valid account holder and allowed to use the mail system.
- **Spam Blocker**—Allows you to specify several ORDB and MAPS RBL type hosts that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these hosts, the message(s) will be refused or flagged.
- **Relay Settings**—Used to control what MDaemon will do when a message arrives at your mail server that is neither from nor to a local address.
- **Trusted Hosts—**Domain names and IP addresses that will be considered as exceptions to the relay rules listed on the Relay Settings tab.
- **Reverse Lookup**—MDaemon can query DNS servers to check the validity of the domain names and addresses reported during incoming messages. Controls on this tab can be used to cause suspicious messages to be refused or a special header inserted into them. Reverse Lookup data will also be reported in the MDaemon logs.

Address Suppression



Domain name: example.com

Select the domain this new suppressed address will apply to.

Email address: spammer@example.net

Wildcards of the form *@domain.com or *@???.com are ok.

□ Refuse to accept mail during SMTP session

□ Inform sender when their mail is rejected

Address suppression works by comparing the address within the email message itself or the address passed in an incoming SMTP session's MAIL parameter to the values configured here. If a match is made the message is rejected. In some cases the message is never accepted in the first place.

Use **Setup | Security Settings | Address Suppression…** to edit the addresses on the suppression list. This list contains addresses that are not allowed to send mail traffic through your server. If a message arrives from an address on this list, it will either be accepted and moved to the bad message queue or refused during the SMTP session and thus never accepted at all, depending upon your settings. This is useful for controlling problem users. Addresses may be suppressed on a per domain basis or globally (applied to all MDaemon domains).

Currently Suppressed Addresses

This window displays all currently suppressed addresses listed by the domain that is suppressing them.

New Suppression Entry

Domain name

Choose the domain to which this suppressed address will apply. In other words, what domain do you want to prevent from receiving mail from the suppressed address? Choose "All Domains" from this list to suppress the address globally.

Note

Messages arriving from addresses listed in the "All Domains" category will be accepted and then moved to the bad message queue. Messages from addresses listed under specific domains will be handled according to that domain's suppression settings. See "*Refuse to accept mail during SMTP session*" and "*Inform sender when their mail is rejected*" below for more suppression options.

Email address
Enter the address that you wish to suppress. Wildcards are accepted, therefore "*@badmail.com" will suppress any message from any user at "badmail.com" and "frank@*" will suppress any message from anyone named "frank", regardless of the domain the message is from.

Remove
Click this button to remove an entry that you have selected in the *Currently Suppressed Addresses* display.

Add
Click this button to add the designated user to the suppression list.

Options

Refuse to accept mail during SMTP session
When this control is enabled, mail to the selected domain from a suppressed address will be refused during the SMTP transaction stage. No mail to that domain from a suppressed address will ever be stored on your server, even in temporary work files. When this control is disabled, messages will be accepted but then moved to the bad message queue. This feature is set on a per domain basis; it is not available for "All Domains" suppressed addresses.

Inform sender when their mail is rejected
If selected, a polite message will be routed back to the suppressed sender telling him or her that their message was deleted. This feature is set on a per domain basis.

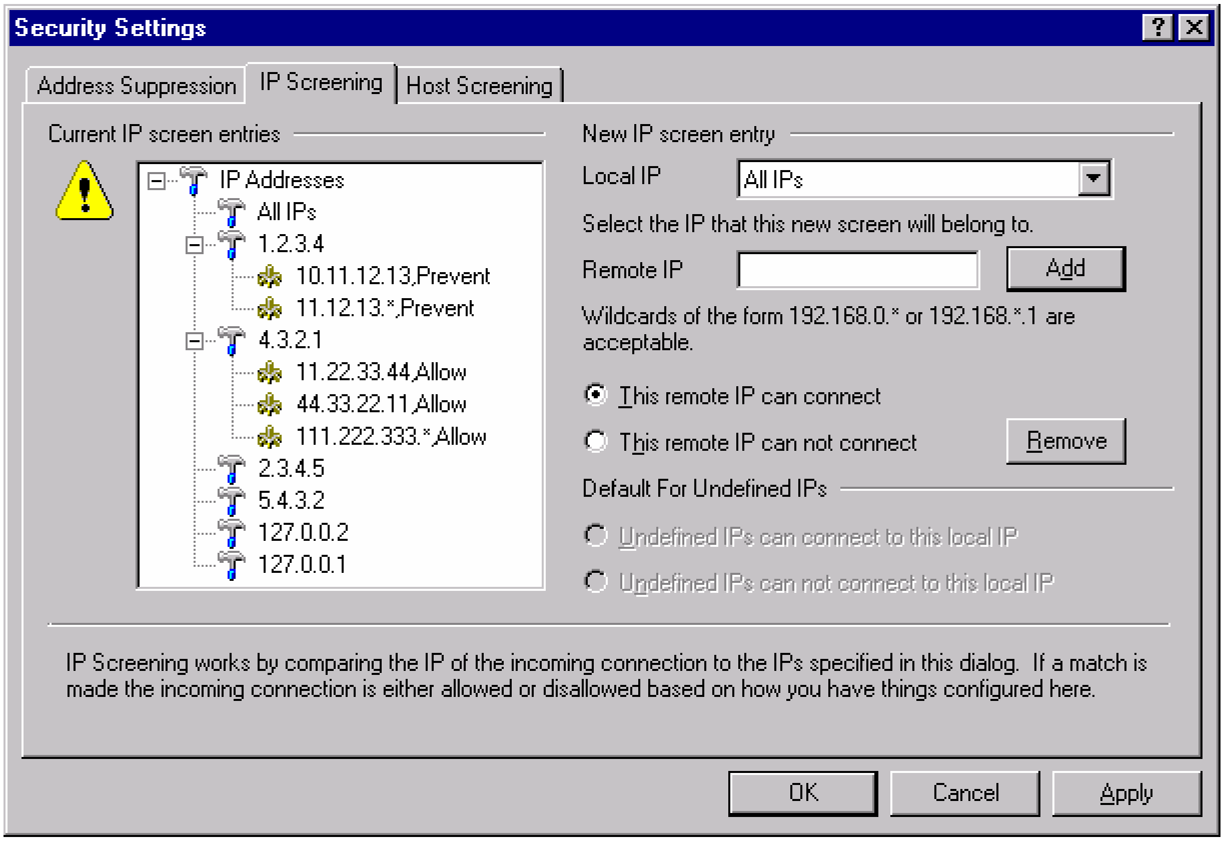
Note

In order for this function to work, a copy of the message must be downloaded during the SMTP session so that it can be parsed. Consequently, this option is incompatible with the "*Refuse to accept mail during SMTP session*" switch.

IP Screening

Use the **Setup|Security Settings|IP Screening…** menu selection to configure IP Screening. The IP Screen is a list of IP addresses that you have designated as either acceptable or non-acceptable. How the server treats attempted connections from the IP addresses listed on the IP Screen depends on the security setting selected in the Screen editor. You may specify a list of IP addresses and then configure the server to only allow connections from those on the list, or you can configure it to abort any connection attempt from an IP address on the list. Wildcards are acceptable in any of the four IP address positions:

..*.*	Matches to any IP address
206.*.*.*	Matches to any IP that begins with 206
206.97.*.239	Matches to IP addresses from 206.97.0.239 to 206.97.255.239



Security Settings

Address Suppression | IP Screening | Host Screening

Current IP screen entries

- IP Addresses
  - All IPs
  - 1.2.3.4
    - 10.11.12.13,Prevent
    - 11.12.13.*,Prevent
  - 4.3.2.1
    - 11.22.33.44,Allow
    - 44.33.22.11,Allow
    - 111.222.333.*,Allow
  - 2.3.4.5
  - 5.4.3.2
  - 127.0.0.2
  - 127.0.0.1

New IP screen entry

Local IP: All IPs

Select the IP that this new screen will belong to.

Remote IP: [Add]

Wildcards of the form 192.168.0.* or 192.168.*.1 are acceptable.

● This remote IP can connect

○ This remote IP can not connect [Remove]

Default For Undefined IPs

○ Undefined IPs can connect to this local IP

○ Undefined IPs can not connect to this local IP

IP Screening works by comparing the IP of the incoming connection to the IPs specified in this dialog. If a match is made the incoming connection is either allowed or disallowed based on how you have things configured here.

Current IP Screen Entries

This window displays all IP addresses that are being screened by MDaemon. They are listed either globally or according to the Local IP Address to which they apply.

New IP Screen Entry

Local IP

Choose from the drop-down list either "All IP's" or the local IP to which you wish to apply the screen.

Remote IP

Enter an IP address that you wish to add to the screened list. You must enter this address in dotted decimal form. The IP Screen works with IP addresses only. Click the *Add* button to add the specified IP address to the address listing.

This remote IP can connect

Selecting this option will allow only those IP addresses specified under the given domain to connect and deliver messages. Attempts to connect via IP addresses not specified in the listing will be refused and immediately aborted. This option is useful for setting up private mail network systems.

This remote IP can not connect

Selecting this option will allow all IP addresses other than those specified in the address listing to connect and deliver messages. Attempts to connect from IP addresses specified in the address listing will be refused and immediately aborted. This option is useful for excluding IP's that cause problems for your mail transport system.

Add

Click this button to add the address specified in the *IP Address* control to the *Current IP Screen Settings* window.

Remove

Click this button to remove a selected entry from the listing.

Default for Undefined IP's

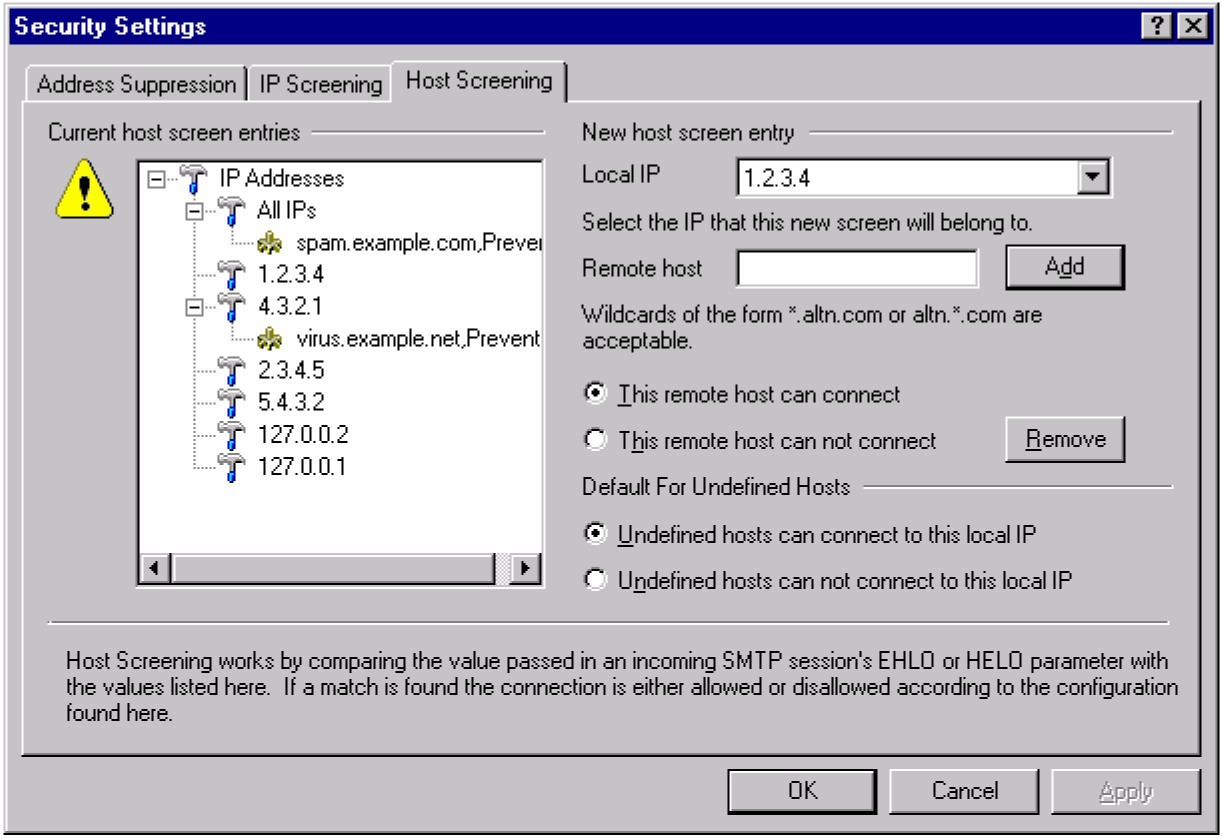
Undefined IPs can connect to this local IP

When this option is chosen, all IP addresses not listed in the IP Screen **will** be allowed to connect.

Undefined IPs cannot connect to this local IP

When this option is chosen, **only** those IP addresses specifically granted permission in the IP Screen will be allowed to connect.

Host Screening



Current host screen entries

- IP Addresses
  - All IPs
    - spam.example.com,Preve
  - 1.2.3.4
  - 4.3.2.1
    - virus.example.net,Prevent
  - 2.3.4.5
  - 5.4.3.2
  - 127.0.0.2
  - 127.0.0.1

New host screen entry

Local IP: 1.2.3.4

Select the IP that this new screen will belong to.

Remote host:

Wildcards of the form *.altn.com or altn.*.com are acceptable.

● This remote host can connect

○ This remote host can not connect

Default For Undefined Hosts

● Undefined hosts can connect to this local IP

○ Undefined hosts can not connect to this local IP

Host Screening works by comparing the value passed in an incoming SMTP session's EHLO or HELO parameter with the values listed here. If a match is found the connection is either allowed or disallowed according to the configuration found here.

Current Host Screen Entries

This window displays all hosts that are being screened by MDaemon. They are listed either globally or according to the Local IP Address to which they apply.

New Host Screen Entry

Local IP

Choose from the drop-down list either "All IP's" or the local IP to which you wish to apply the screen. This is the IP address that the remote host is attempting to connect to.

Remote host

Enter a host that you wish to add to the screened list. Wildcards are permitted, so you could enter "`*.example.com`" to prevent or allow connections from all sub domains of example.com, or "`example.*`" to apply the screen to all top-level domains beginning with "`example`". Click the *Add* button to add the specified host to the list.

This remote host can connect

Selecting this option will allow only those host specified under the given domain to connect and deliver messages. Attempts to connect by hosts not specified in the listing will be refused and immediately aborted. This option is useful for setting up private mail network systems.

This remote host can not connect
Selecting this option will allow all host other than those specified in the address listing to connect and deliver messages. Attempts to connect by a host specified in the address listing will be refused and immediately aborted. This option is useful for excluding hosts that cause problems for your mail transport system.

Add
Click this button to add the host to the list.

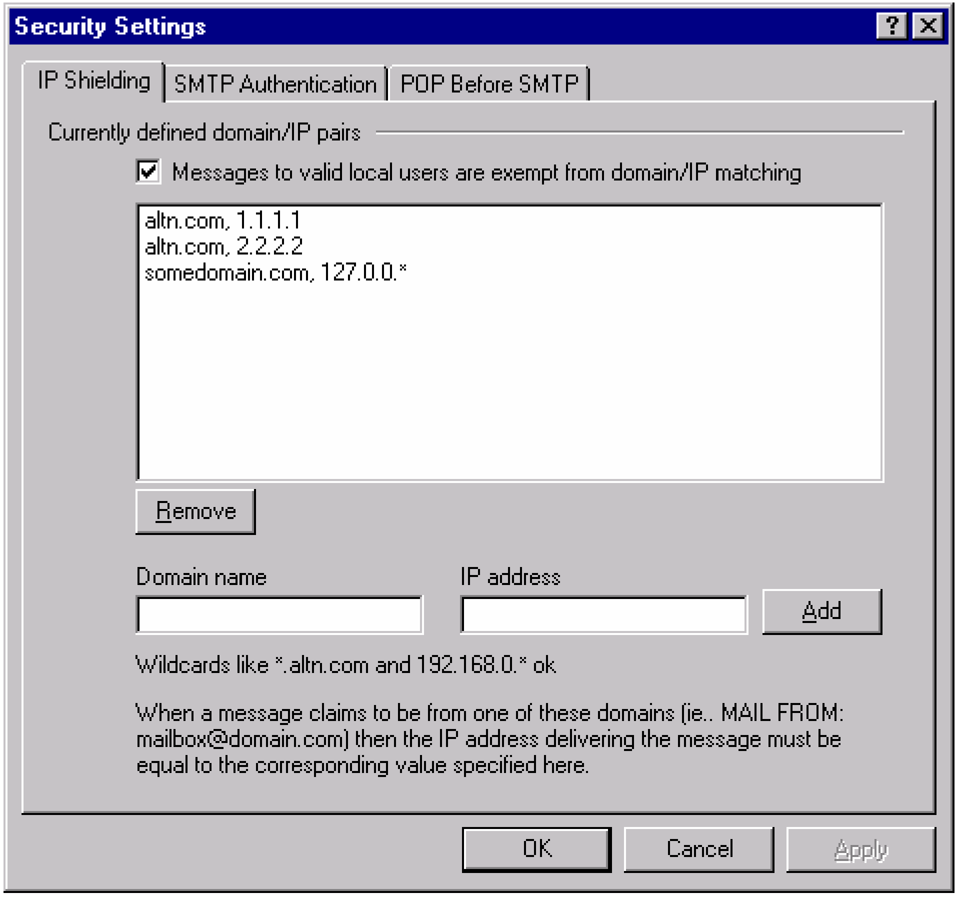
Remove
Click this button to remove a selected entry from the list.

Default for Undefined Hosts

Undefined hosts can connect to this local IP
When this option is chosen, all hosts not listed in the host screen **will** be allowed to connect to the specified IP address.

Undefined hosts cannot connect to this local IP
When this option is chosen, **only** those hosts specifically granted permission in the host screen will be allowed to connect to the specified IP address.

IP Shielding



Currently defined domain/IP pairs

☑ Messages to valid local users are exempt from domain/IP matching

altn.com, 1.1.1.1
altn.com, 2.2.2.2
somedomain.com, 127.0.0.*

Domain name

IP address

Wildcards like *.altn.com and 192.168.0.* ok

When a message claims to be from one of these domains (ie.. MAIL FROM: mailbox@domain.com) then the IP address delivering the message must be equal to the corresponding value specified here.

Use the **Setup→Security Settings→IP Shielding…** menu selection to configure IP Shielding. The IP Shield is a list of domain names and matching IP addresses that will be checked during the `SMTP MAIL FROM:` command. An SMTP session claiming to be from someone at one of the listed domains will be honored only if it is coming from a machine with one of the associated IP addresses. For example, suppose your domain name is mdaemon.com and your local LAN computers use IP addresses in the range from 192.168.0.0 to 192.168.0.255. With this information you can set up IP Shielding to associate the domain name mdaemon.com with the IP address range 192.168.0.* (wildcards are allowed). Thus anytime a computer connects to your SMTP server and states, "`MAIL FROM <someone@mdaemon.com>`", the SMTP session will continue only if the connecting computer has an IP address within the required range from 192.168.0.0 to 192.168.0.255.

Currently Defined Domain/IP Pairs

This is the list of domain names and their corresponding IP addresses that will be compared when someone attempts to connect to MDaemon claiming to be from one of them.

Messages to valid local users are exempt from domain/IP matching

Click this option if you want only those messages that are destined for a non-local user or invalid local user to be checked for a domain/IP match. This will prevent others from posing as one of your local users in order to relay their mail **through** your server but save resources by not checking those sending messages **to** users on your server.

Domain name

Enter the domain name that you wish to associate with a specific IP address range.

IP address

Enter the IP address that you wish to associate with a domain name. You must enter this address in dotted decimal form.

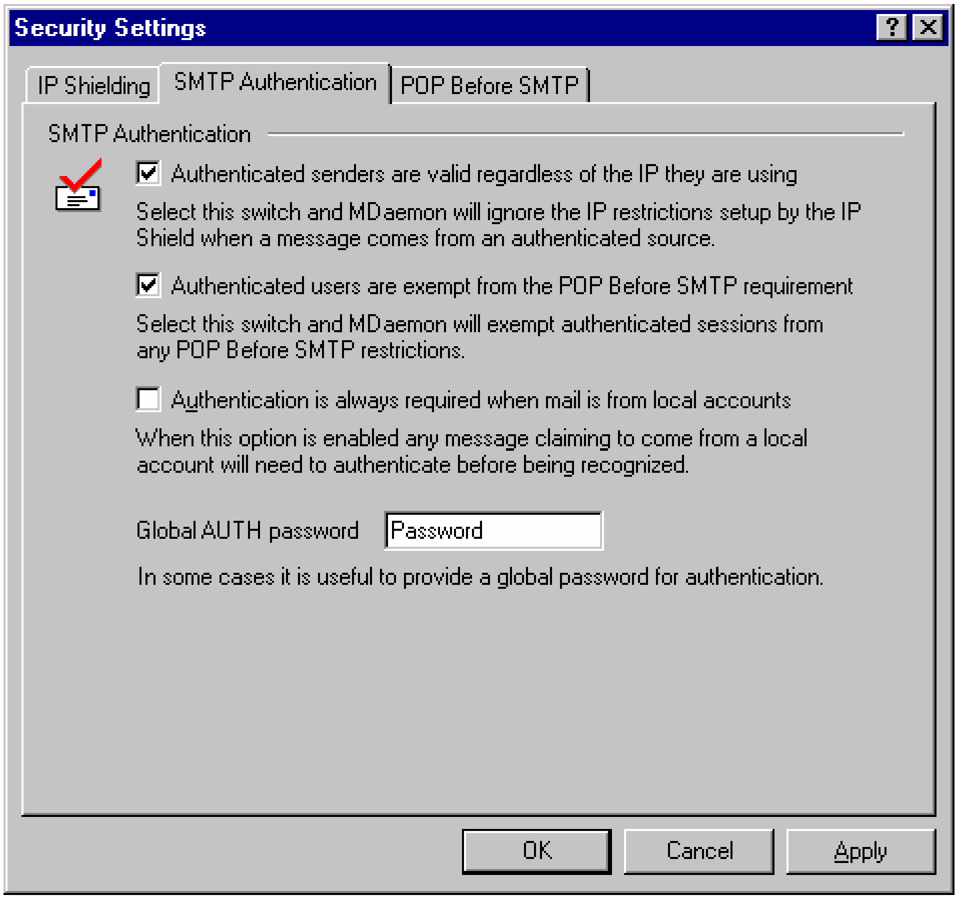
Add

Click the *Add* button to add the domain and IP address range to the listing.

Remove

Click this button to remove the selected entries from the listing.

SMTP Authentication



SMTP Authentication

☑ Authenticated senders are valid regardless of the IP they are using

Select this switch and MDaemon will ignore the IP restrictions setup by the IP Shield when a message comes from an authenticated source.

☑ Authenticated users are exempt from the POP Before SMTP requirement

Select this switch and MDaemon will exempt authenticated sessions from any POP Before SMTP restrictions.

□ Authentication is always required when mail is from local accounts

When this option is enabled any message claiming to come from a local account will need to authenticate before being recognized.

Global AUTH password: Password

In some cases it is useful to provide a global password for authentication.

SMTP Authentication

Authenticated senders are valid regardless of the IP they are using

When this control is active, currently shielded IP addresses will not apply to users that have been authenticated. Mail will be accepted from them regardless of the IP address from which they are connecting.

Authenticated users are exempt from the POP before SMTP requirement

If you are utilizing the POP before SMTP security feature below, you may click this control to make authenticated users exempt from this restriction. An authenticated user will not need to check his or her email before sending messages.

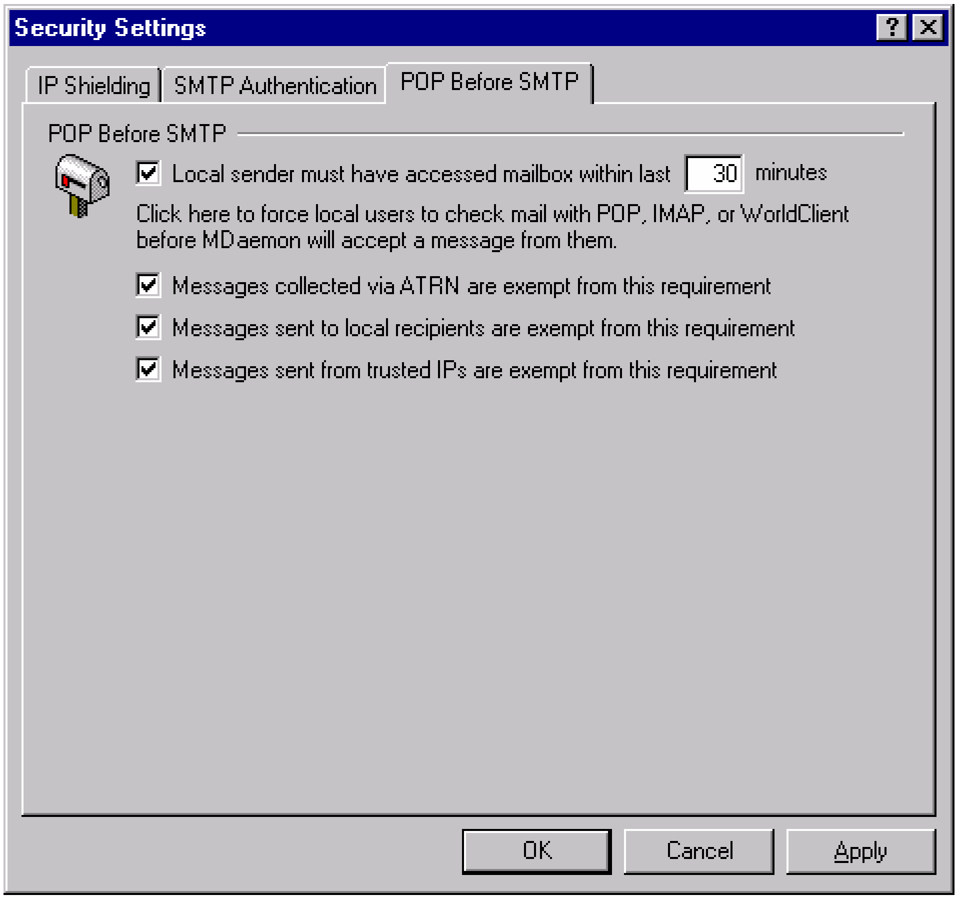
Authentication is always required when mail is from local accounts

If the person sending a message claims to be from one of MDaemon’s domains, the account must first be authenticated or MDaemon will refuse to accept the message for delivery.

Global AUTH password

If the *Authenticated senders are valid regardless of the IP they are using* control is enabled, MDaemon accounts configured for dynamic NT authentication must use this global AUTH password for authentication instead of their normal NT password.

POP Before SMTP



POP Before SMTP

☑ Local sender must have accessed mailbox within last 30 minutes

Click here to force local users to check mail with POP, IMAP, or WorldClient before MDaemon will accept a message from them.

☑ Messages collected via ATRN are exempt from this requirement

☑ Messages sent to local recipients are exempt from this requirement

☑ Messages sent from trusted IPs are exempt from this requirement

POP Before SMTP

Local sender must have accessed mailbox within last [XX] minutes

With this feature enabled, whenever someone claims to be a local user they must have logged in and checked their local mailbox within the specified number of minutes before they will be allowed to send mail.

Messages collected via ATRN are exempt from this requirement

Click this control if you want messages collected via ATRN to be exempt from the POP Before SMTP requirement.

Messages sent to local recipients are exempt from this requirement

Click this checkbox if you want messages that are sent from one local user to another to be exempt from the "Local sender must have accessed mailbox…" requirement. Ordinarily, MDaemon will enforce the "POP before SMTP" requirement as soon as the sender is known, but when this control is enabled MDaemon will wait until the recipient of the message is revealed before determining whether or not it is required.

Messages sent from trusted IPs are exempt from this requirement

If this checkbox is enabled, messages arriving from a domain listed in the *Currently defined domain/IP pairs* area of this dialog will be exempt from the *Local sender must have accessed mailbox…* requirement.

Spam Blocker

Spam Blocker can be used to prevent most “spam” email from reaching your users. This new security feature allows you to specify several ORDB and MAPS RBL type hosts (which maintain lists of servers known to relay “spam”) that will be checked each time someone tries to send a message to your server. If the connecting IP has been blacklisted by any one of these hosts, the message(s) will be refused or flagged.

> **Note**
>
> Use of this feature can prevent most spam from being sent to your users. However, some sites are blacklisted by mistake and therefore using this feature could cause some difficulties, but it is worthwhile if you are worried about controlling spam.
>
> Spam Blocker lookups are performed using the DNS server specified in **Setup|Primary Domain…|DNS**. This feature was tested and performed well with no significant delay per mail session.

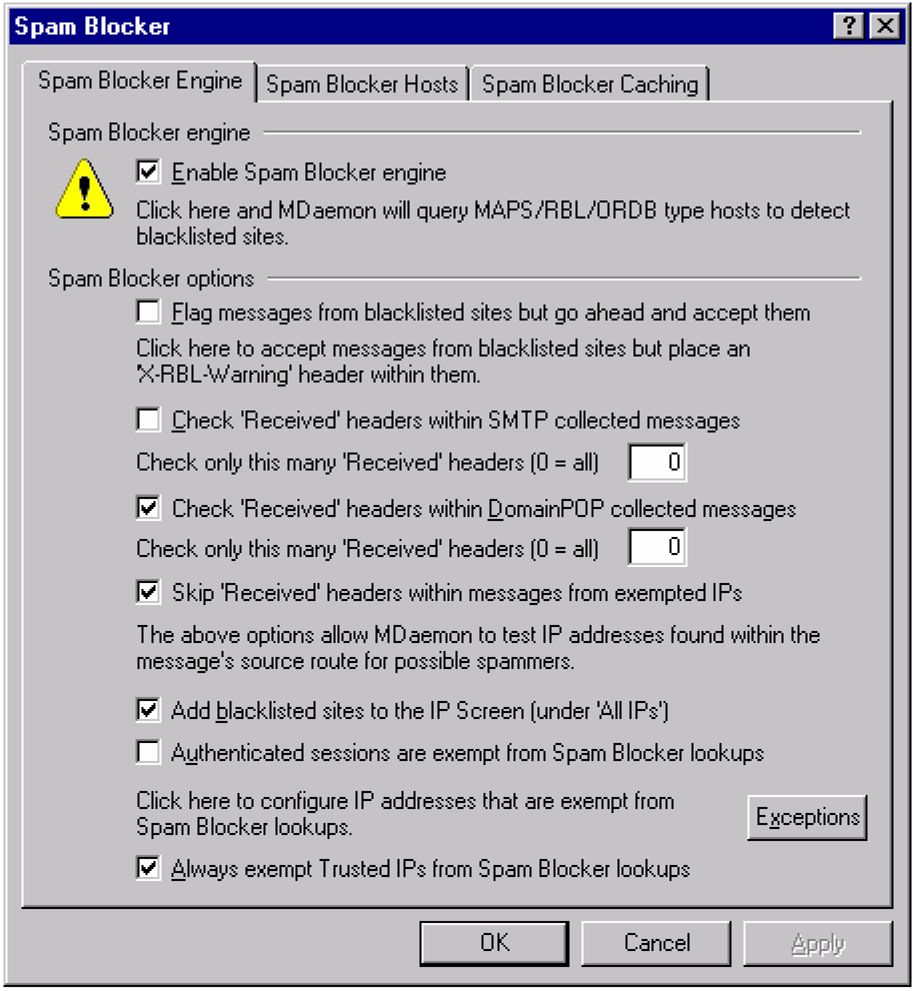
Spam Blocker includes an “exception” database for designating IP addresses that will not be subject to Spam Blocker lookups. Before activating this feature, you should add your local IP address range to the exception list to prevent lookups on it. 127.0.0.1 is exempt and therefore doesn’t need to be added to the exceptions.

For information on spam and how to control and eliminate it using ORDB and MAPS RBL, visit:

```
http://www.ordb.org
http://www.mail-abuse.com/rbl/
```

ORDB and MAPS RBL are trademarks of their respective organizations. Alt-N Technologies is proud to be associated with them and make use of their services on behalf of our customers.

Spam Blocker Engine



Spam Blocker

Spam Blocker Engine | Spam Blocker Hosts | Spam Blocker Caching

Spam Blocker engine

☑ Enable Spam Blocker engine

Click here and MDaemon will query MAPS/RBL/ORDB type hosts to detect blacklisted sites.

Spam Blocker options

□ Flag messages from blacklisted sites but go ahead and accept them

Click here to accept messages from blacklisted sites but place an 'X-RBL-Warning' header within them.

□ Check 'Received' headers within SMTP collected messages

Check only this many 'Received' headers (0 = all) 0

☑ Check 'Received' headers within DomainPOP collected messages

Check only this many 'Received' headers (0 = all) 0

☑ Skip 'Received' headers within messages from exempted IPs

The above options allow MDaemon to test IP addresses found within the message's source route for possible spammers.

☑ Add blacklisted sites to the IP Screen (under 'All IPs')

□ Authenticated sessions are exempt from Spam Blocker lookups

Click here to configure IP addresses that are exempt from Spam Blocker lookups.

☑ Always exempt Trusted IPs from Spam Blocker lookups

Spam Blocker Engine

Enable Spam Blocker engine

Click this checkbox to turn on Spam Blocker.

Spam Blocker Options

Flag messages from blacklisted sites but go ahead and accept them

When this control is enabled, MDaemon will not refuse messages that receive a blacklisted result. However, those messages will have an `X-RBL-Warning:` header inserted. You can then use the Content Filter feature to search for messages with this header and do with them as you please.

Check 'Received' headers within SMTP collected messages

Click this switch if you want Spam Blocker to check the IP address stamped in the "`Received`" headers of messages received via SMTP.

Check only this many 'Received' headers (0 = all)

Specify the number of 'Received' headers that you want Spam Blocker to check starting with the most recent. A value of "0" means that all 'Received' headers will be checked.

Check 'Received' headers within DomainPOP collected messages
When this switch is enabled Spam Blocker will check the IP address stamped in the "`Received`" headers of downloaded messages.

Check only this many 'Received' headers (0 = all)
Specify the number of 'Received' headers that you want Spam Blocker to check starting with the most recent. A value of "0" means that all 'Received' headers will be checked.

Skip 'Received' headers within messages from exempted IPs
When this option is enabled, Spam Blocker will not check the "Received" headers within messages coming from IP addresses that you have designated as exceptions. Click the "Exceptions" button below to designate those IP addresses.

Add blacklisted sites to the IP Screen (under All Domains)
When a Spam Blocker lookup determines that a site is blacklisted, MDaemon will add it to the IP Screen if this control is enabled. Adding its IP address to the IP Screen will prevent it from ever connecting to your MDaemon in the future.

Caution!

Hosts that are blacklisted will oftentimes correct whatever problem there was which caused them to obtain the blacklisted status in the first place. If a blacklisted IP address is added to the IP Screen then MDaemon will never accept connections from that IP address again -- even if they correct the problem and are no longer blacklisted by the Spam Blocker Hosts. You should therefore be aware that use of this feature could potentially prevent a valid host from connecting to you.

Authenticated sessions are exempt from Spam Blocker lookups
Click this checkbox if you want those sessions that were authenticated using the AUTH command to be exempt from Spam Blocker lookups. It will perform no lookups for those sessions.

For more information see:

On-Demand Mail Relay—page 51

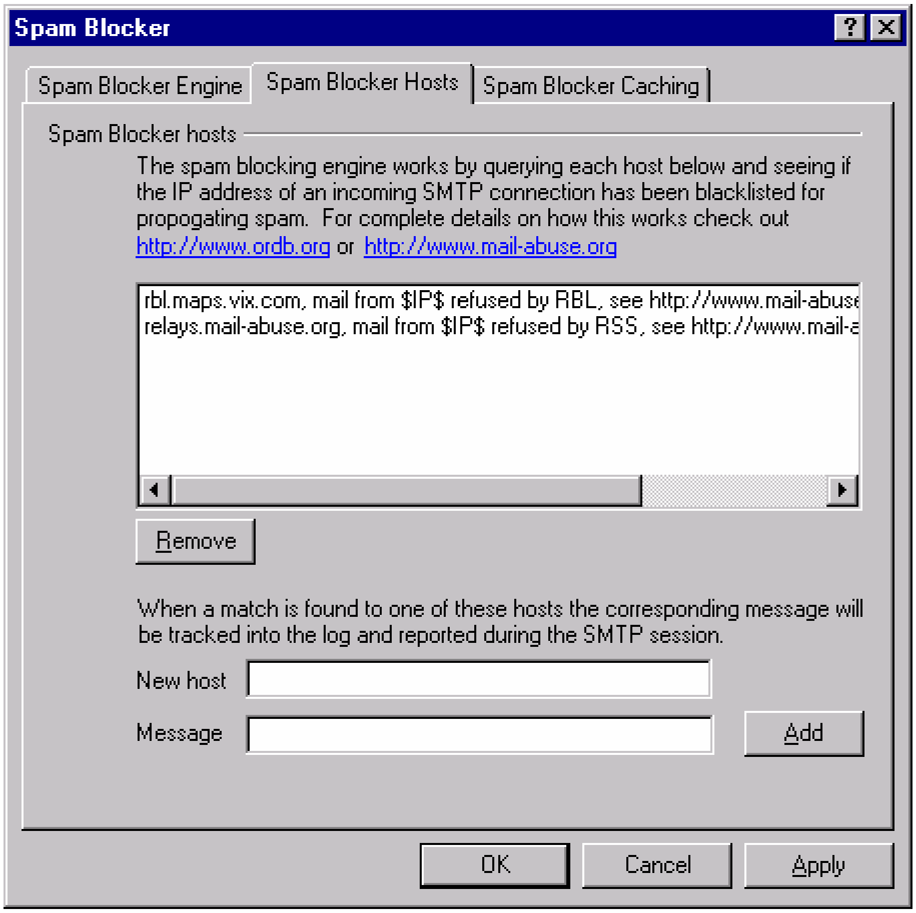
IP Shielding—page 115

Domain Gateways—page 289

Always exempt Trusted IPs from Spam Blocker lookups
Click this checkbox if you want addresses that are listed on the Trusted Hosts tab of Relay Settings (see page 127) to be exempt from Spam Blocker lookups.

Exceptions
Click this button to open the Spam Blocker Exceptions dialog on which you can designate IP addresses that will be exempt from Spam Blocker lookups. You should always include your local IP address range to prevent lookups on it. 127.0.0.1 is already exempt and therefore doesn't need to be added to the list.

Spam Blocker Hosts



Spam Blocker hosts

The spam blocking engine works by querying each host below and seeing if the IP address of an incoming SMTP connection has been blacklisted for propogating spam. For complete details on how this works check out http://www.ordb.org or http://www.mail-abuse.org

```
rbl.maps.vix.com, mail from $IP$ refused by RBL, see http://www.mail-abuse
relays.mail-abuse.org, mail from $IP$ refused by RSS, see http://www.mail-a
```

When a match is found to one of these hosts the corresponding message will be tracked into the log and reported during the SMTP session.

Spam Blocker Hosts

MDaemon will query each of these hosts when performing a Spam Blocker lookup on an IP address. If a host replies to the query with a positive result, MDaemon will refuse to accept the message from that IP address, and will also send the short message associated with the host that blacklisted the address.

Remove

Select an entry from the Spam Blocker Hosts list and click this button to remove it from the list.

New host

If you wish to add a new host to be queried for blacklisted IP addresses, enter it here.

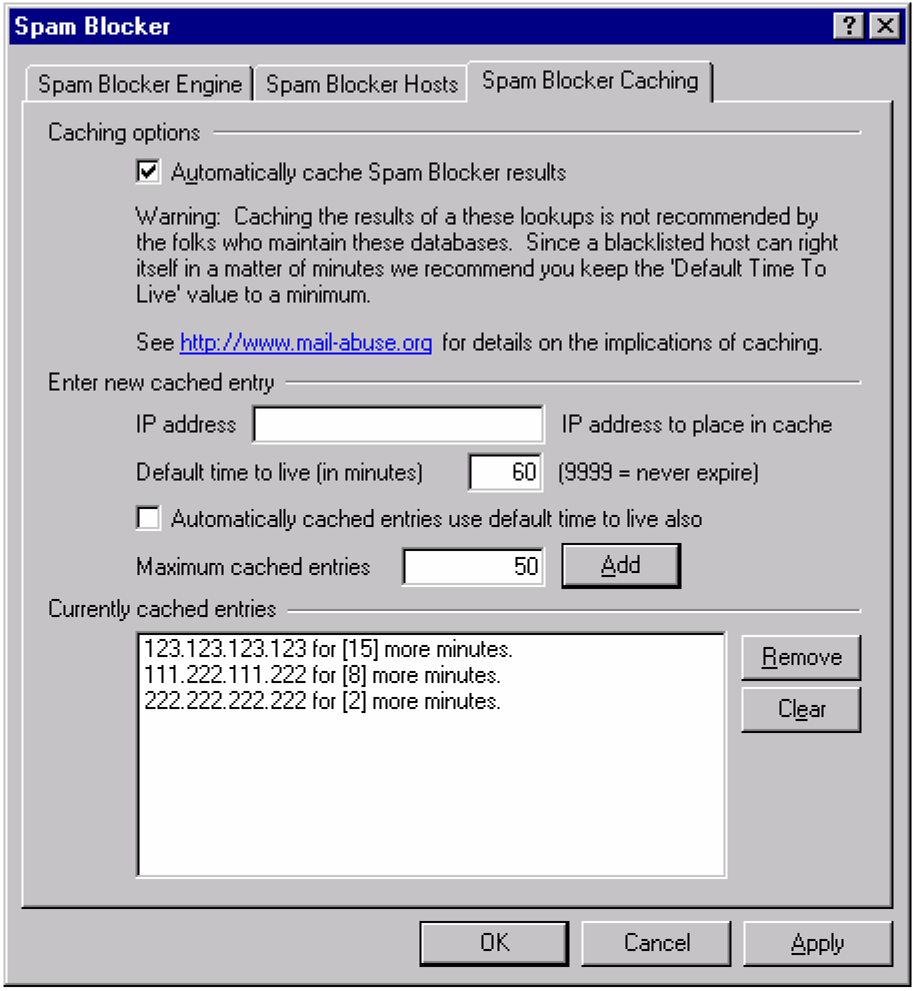
Message

This is the message that will be sent when an IP address has been blacklisted by the *New Host*.

Add

After entering a *New Host* and *Message*, click this button to add it to the Spam Blocker Hosts list.

Spam Blocker Caching



☑ Automatically cache Spam Blocker results

Warning: Caching the results of a these lookups is not recommended by the folks who maintain these databases. Since a blacklisted host can right itself in a matter of minutes we recommend you keep the 'Default Time To Live' value to a minimum.

See http://www.mail-abuse.org for details on the implications of caching.

IP address [ ] IP address to place in cache

Default time to live (in minutes) 60 (9999 = never expire)

☐ Automatically cached entries use default time to live also

Maximum cached entries 50

```
123.123.123.123 for [15] more minutes.
111.222.111.222 for [8] more minutes.
222.222.222.222 for [2] more minutes.
```

Spam Blocker Caching Engine

Automatically cache Spam Blocker results

Enable this control if you want to cache those IP addresses that receive a positive (i.e. blacklisted) result from a Spam Blocker lookup.

Warning!

Although caching addresses may conserve some resources—since Spam Blocker lookups will not need to be performed on those IP addresses that have already been cached—it is not recommended by the Spam Blocker Hosts. Since a blacklisted IP address could have its status corrected in a matter of minutes, caching entries could result in mail being refused unnecessarily. Caution should therefore be used when caching entries. If you choose to use this feature then we recommend keeping small the amount of time that any given entry is cached. For more information on the implications of caching Spam Blocker lookups, see: www.mail-abuse.org.

Enter New Cached Entry

IP address
Enter the IP address that you wish to manually add to the Spam Blocker cache.

Default time to live (in minutes)
This is the amount of time that the entry will remain in the Spam Blocker cache. Entering 9999 into this field will prevent the entry from expiring—however this is not recommended.

Automatically cached entries use default time to live also
Click this check box if you want automatically cached entries to use the *Default time to live* setting specified above. Normally the time to live (TTL) parameter is based on information returned during the DNS lookup rather than by the *Default time to live* setting.

Maximum cached entries
This is the maximum number of entries that you want to allow to be cached.

Add
After entering the *IP Address* and *Default Time To Live* click this button to add the entry to the list of cached IP addresses.

Currently cached entries
This box list the IP addresses that are currently cached. MDaemon will not perform a lookup on them. They will be treated as blacklisted addresses.

Remove
Select an entry and then click this button to remove it from the list of cached addresses.

Clear
Click this button the clear the list of all cached IP addresses.

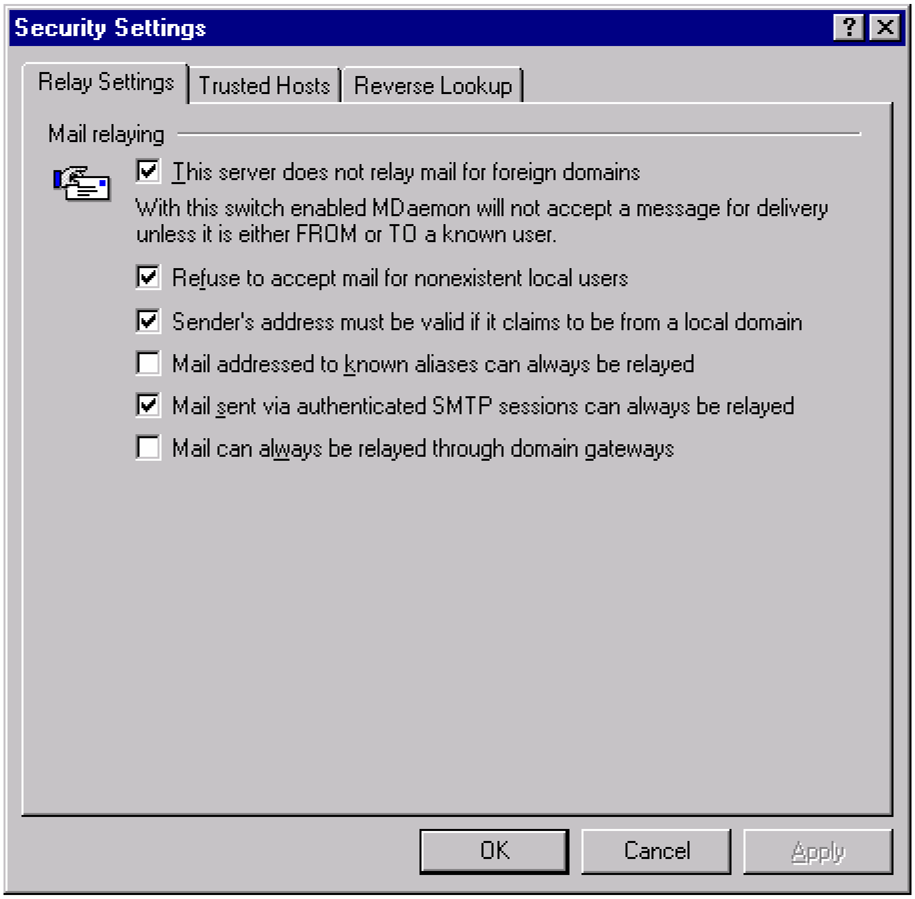
Relay Settings

Use the **Setup→Security Settings→Relay Control…** menu selection to define how your server reacts to mail relaying. When a message arrives at your mail server that is neither from nor to a local address, your server is being asked to relay (or deliver) the message on behalf of another user. If you do not want your server to relay mail for unknown users you can use the settings provided here.

Warning!

Relaying email indiscriminately for other servers could result in your domain being blacklisted by one or more Spam Blocker hosts (see page 119). Open relaying is greatly discouraged because "spammers" exploit open servers to "hide their tracks".

Relay Settings



Security Settings

Mail relaying

☑ This server does not relay mail for foreign domains

With this switch enabled MDaemon will not accept a message for delivery unless it is either FROM or TO a known user.

☑ Refuse to accept mail for nonexistent local users

☑ Sender's address must be valid if it claims to be from a local domain

□ Mail addressed to known aliases can always be relayed

☑ Mail sent via authenticated SMTP sessions can always be relayed

□ Mail can always be relayed through domain gateways

Mail Relay Control

This server does not relay mail for foreign domains

When this switch is selected, MDaemon will refuse to accept messages for delivery that are both FROM and TO a non-local user.

Refuse to accept mail for nonexistent local users

When this checkbox is enabled, MDaemon will refuse to accept mail that is for a local domain but addressed to a nonexistent user. "Local" includes both LAN and Domain Gateways.

Sender's address must be valid if it claims to be from a local domain

If the person sending a message claims to be from one of MDaemon's domains, the account used will be verified against the account database. The local account must exist or MDaemon will refuse to accept the message for delivery.

Mail addressed to known aliases can always be relayed

Click this control if you want MDaemon to relay mail for Address Aliases (page 256) regardless of your Relay Control settings.

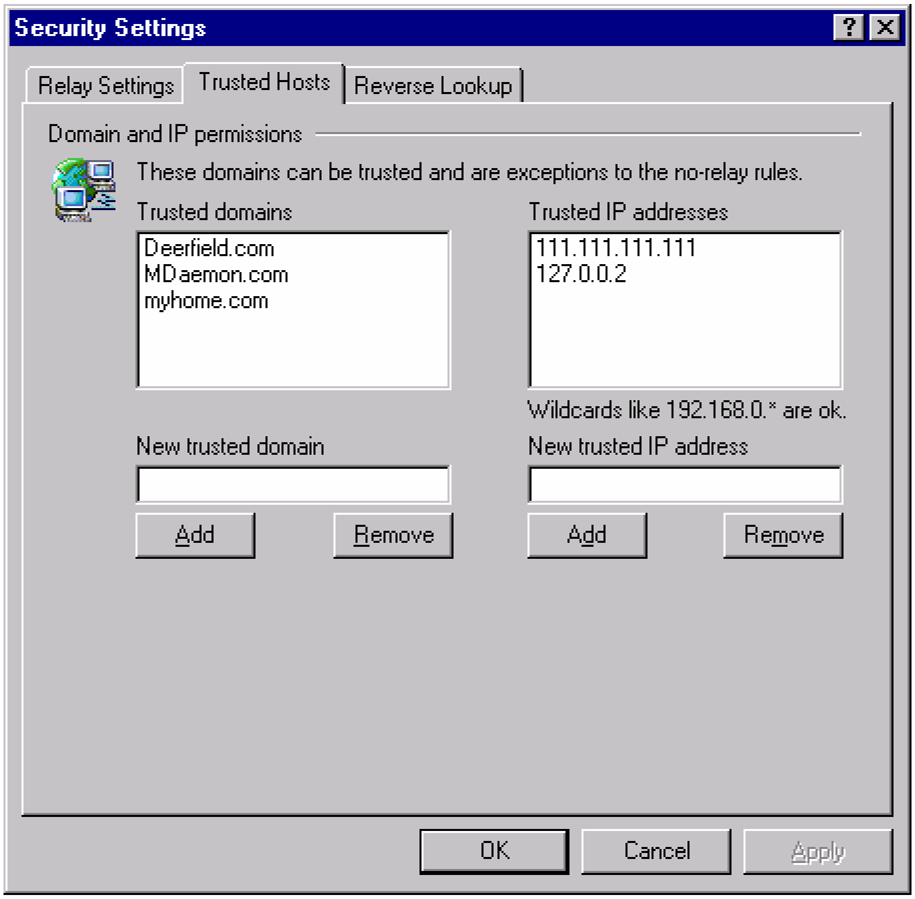
Mail sent via authenticated SMTP sessions can always be relayed

When this checkbox is enabled, MDaemon will always relay mail when it is sent via an authenticated SMTP session.

Mail can always be relayed through domain gateways

Enable this checkbox if you want MDaemon to permit mail relaying through domain gateways regardless of your Relay Control settings. This feature is disabled by default and isn't recommended.

Trusted Hosts



These domains can be trusted and are exceptions to the no-relay rules.

Trusted domains

Deerfield.com
MDaemon.com
myhome.com

Trusted IP addresses

111.111.111.111
127.0.0.2

Wildcards like 192.168.0.* are ok.

Domain and IP Permissions

Trusted domains
Domains that you list here are exceptions to the no-relay rule. These domains are "trusted" by your server and MDaemon will not refuse to relay mail for their users.

New trusted domain
Enter a new domain name to be added to the *Trusted Domains* list.

Add
Click this button to add the new domain to the *Trusted Domains* list.

Remove
Click this button to remove the selected entries from the *Trusted Domains* list.

Trusted IP addresses
IP addresses that you list here are exceptions to the no-relay rule. These IP addresses are "trusted" by your server and MDaemon will not refuse to relay mail for their users.

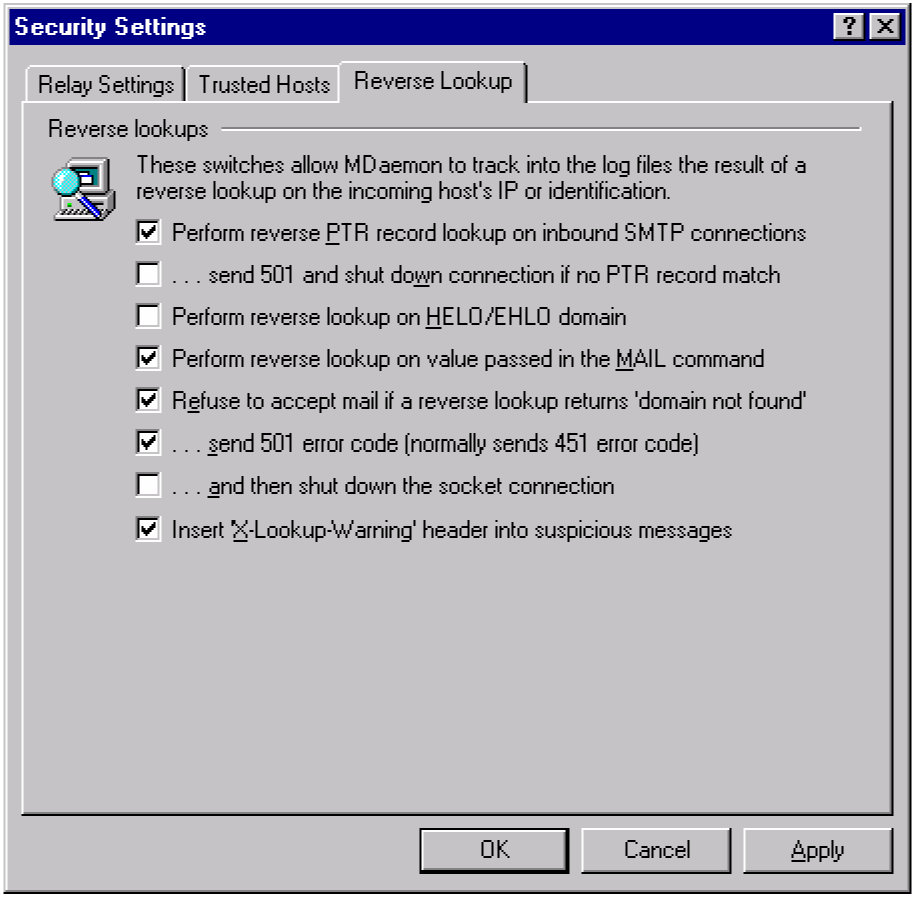
New trusted IP address

Enter a new IP address to be added to the *Trusted IP Addresses* list.

Add
Click this button to add the new IP address to the *Trusted IP Addresses* list.

Remove
Click this button to remove the selected entries from the *Trusted IP Addresses* list.

Reverse Lookup



Reverse lookups

These switches allow MDaemon to track into the log files the result of a reverse lookup on the incoming host's IP or identification.

☑ Perform reverse PTR record lookup on inbound SMTP connections

□ . . . send 501 and shut down connection if no PTR record match

□ Perform reverse lookup on HELO/EHLO domain

☑ Perform reverse lookup on value passed in the MAIL command

☑ Refuse to accept mail if a reverse lookup returns 'domain not found'

☑ . . . send 501 error code (normally sends 451 error code)

□ . . . and then shut down the socket connection

☑ Insert 'X-Lookup-Warning' header into suspicious messages

Using the controls on this tab MDaemon can be configured to do a reverse lookup on the domain passed in the HELO/EHLO and/or MAIL commands. When performing the lookups MDaemon will attempt to acquire all of the MX and A record IP addresses for the given domain. Then the IP of the machine making the connection is compared to this list in an attempt to determine whether the sender might be forging their identity.

Oftentimes the sending mail server's IP address will not match any known MX or A records for a given domain and yet still be delivering the mail legitimately. The purpose of the Reverse Lookup process is therefore not to exclude mail but to include as much information as possible in the log files, and to provide the means whereby the postmaster can act according to their own local policies regarding these suspicious messages. To that end, an option exists that makes it possible for a special header to be inserted into all messages that do not pass a reverse lookup. The content filter system can then be used to determine the fate of messages containing the header.

You can also perform reverse lookups on pointer (PTR) records of incoming IP addresses. When using this option the connection can be aborted or a warning header inserted into the message if the incoming IP address does not match any PTR record.

Finally, it is generally agreed that accepting mail from sources that identify themselves by using a domain that does not exist should be optional. Therefore, a switch exists that makes it possible for you to refuse messages for which the reverse lookup process returns a "domain not found" message from the DNS server. In such cases, MDaemon will return a `451` error code, refuse to accept the message, and then allow the SMTP session to progress. However, should you wish to return a `501` error code, close the socket connection, or do both, other switches are provided for those purposes.

Trusted IP addresses and localhost (127.0.0.1) are always exempt from reverse lookups.

Reverse Lookups

Perform reverse PTR record lookup on inbound SMTP connections
Enable this option if you want MDaemon to perform reverse pointer record lookups on all inbound SMTP connections.

…send 501 and shut down connection if no PTR record match
If this box is checked then MDaemon will send a `501` error code (syntax error in parameters or arguments) and shut down the connection if the result of a reverse pointer record lookup fails to match.

Perform reverse lookup on HELO/EHLO domain
Click this box if you want a reverse lookup to be performed on the domain name that is reported during the `HELO/EHLO` portion of the session. The `HELO/EHLO` command is used by the client (sending machine) to identify itself to the server. The domain name passed by the client in this command is used by the server to populate the `from` portion of the `Received` header.

Perform reverse lookup on value passed in the MAIL command
Enabling this switch will cause a reverse lookup to be performed on the domain name that is passed during the `MAIL` command portion of the mail transaction. The address passed in the `MAIL` command is supposed to be the reverse-path for the message, and is usually the mailbox from which the message is originating. Sometimes, however, it is the address to which error messages should be directed instead.

Refuse to accept mail if a reverse lookup returns 'domain not found'
When a lookup results in "`domain not found`", enabling this option will cause the message to be refused with a `451` error code (Requested action aborted: local error in processing) and then the session will be allowed to progress normally to its conclusion.

…send 501 error code (normally sends 451 error code)
Enable this checkbox if you want the error code that is sent in response to a "domain not found" result to be `501` (syntax error in parameters or arguments) instead of `451`.

…and then shut down the socket connection
Click this checkbox if you want the connection to be shutdown immediately instead of allowed to progress when "`domain not found`" is the result of the reverse lookup.

Insert 'X-Lookup-Warning' header into suspicious messages
Click this checkbox if you want a header to be inserted into messages that are considered suspicious due to the results of the reverse lookup. You can edit the name and content of the header by editing the following MDaemon.ini key:

```
[Special]
LookupWarningHeader=X-LookupWarning: text
```

If you edit this value, MDaemon will allow you to make the “X-LookupWarning: text” portion anything that you want, but be certain that your alterations conform to RFC regulations regarding mail headers.

Chapter

10

Header Translation

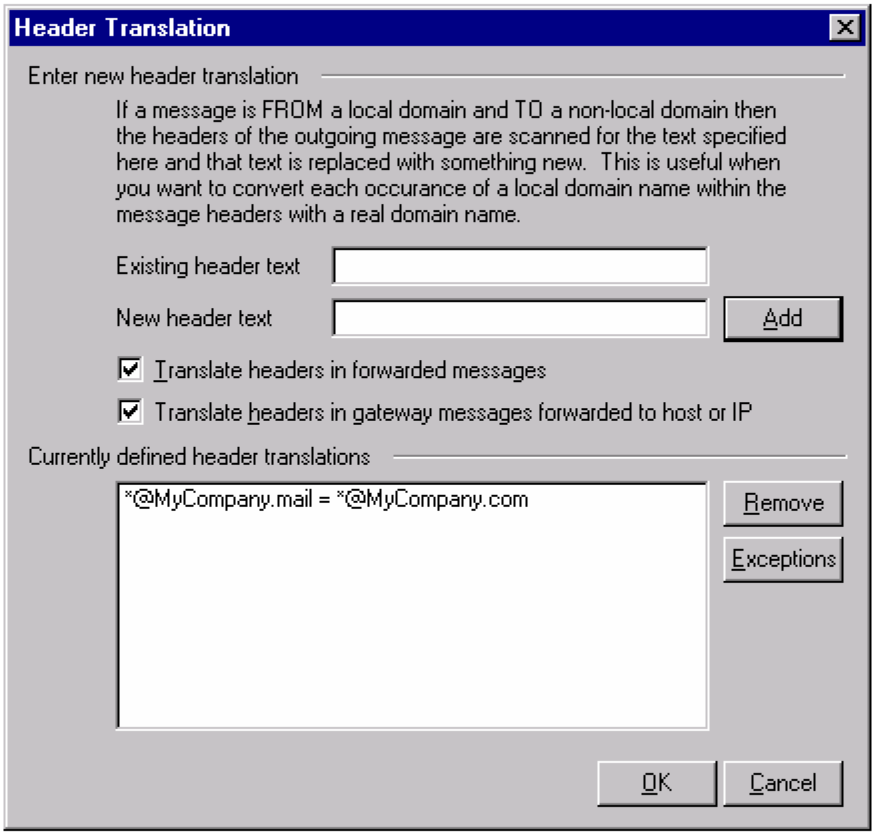
Changing header text on the fly.

The "Outbound Domain Conversion" feature has been replaced with the "Header Translation" feature. This new dialog can change any portion of text found within a header to a new value, whenever a message is detected which must leave your domain and travel across the Internet. Your old "Outbound Domain Conversion" settings will be migrated to this new "Header Translation" feature. It works like this: You specify the text you want to search for and its corresponding replacement value. MDaemon will then search through all the headers in the message and make the replacements. You may also specify headers that MDaemon should **not** modify (such as "Subject:" or "Received:" headers) by clicking the "Exceptions" button on this dialog.

This feature is necessary for some MDaemon configurations in which the local domain name is fictitious or different from the domain name that must appear on outbound mail. In such a situation, Header Translation could be used to change every occurrence of "@localdomain.com" to "@RemoteDomain.com".

This feature is much more powerful and versatile than the old "Outbound Domain Conversion" feature while retaining the same basic functionality.

Header Translation



Header Translation

Enter new header translation

If a message is FROM a local domain and TO a non-local domain then the headers of the outgoing message are scanned for the text specified here and that text is replaced with something new. This is useful when you want to convert each occurance of a local domain name within the message headers with a real domain name.

Existing header text

New header text

☑ Translate headers in forwarded messages

☑ Translate headers in gateway messages forwarded to host or IP

Currently defined header translations

*@MyCompany.mail = *@MyCompany.com

Enter New Header Translation

Existing header text
Type the text that you want to be replaced when it is found within the headers of any outbound message.

New header text
This text will be substituted for that which you specified in the *Existing Header Text* field.

Add
Click this button to add the above text parameters to the Current Header Translations list.

Translate headers in forwarded messages
Click this checkbox to cause the header translations to apply also to messages automatically forwarded from a local domain to a non-local domain.

Translate headers in gateway messages forwarded to host or IP
Click this check box if you want the headers to be translated in forwarded domain gateway mail. See the Mail Forwarding tab of the Gateway Editor (page 296) for more information.

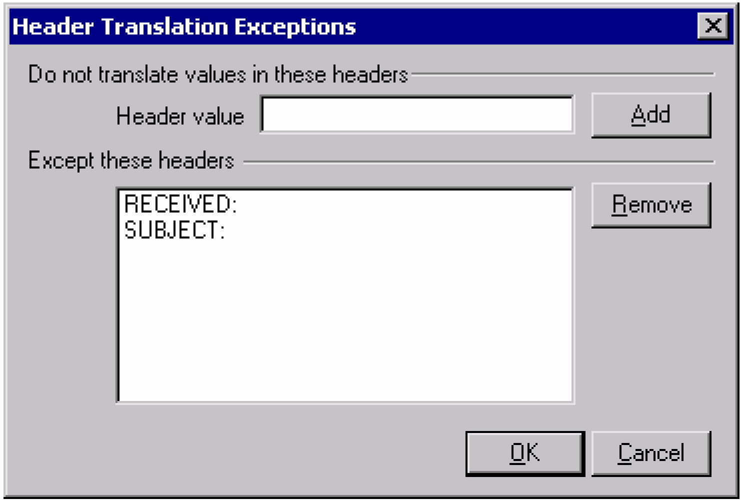
Currently Defined Header Translations

This list contains the portions of text that MDaemon will scan for in the outbound message headers, and the text that will be substituted when a match is found.

Remove
Select an entry in the Current Header Translations list and then click this button to remove it from the list.

Exceptions
Click this button to open the Header Translation Exceptions dialog. This dialog is used for specifying any Headers that you wish to be omitted from the Header Translation process.

Header Translation Exceptions


Header Translation Exceptions
Do not translate values in these headers
Header value
Add
Except these headers
Remove
OK
Cancel

RECEIVED:
SUBJECT:

Do Not Translate Values in These Headers

Header value
Enter any header that you want to be omitted from the Header Translation process.

Add
Click this button to add a new header to the list.

Except These Headers

MDaemon will not scan these headers when it is substituting header text.

Remove
Select a header in the list and then click this button to remove it.

Chapter

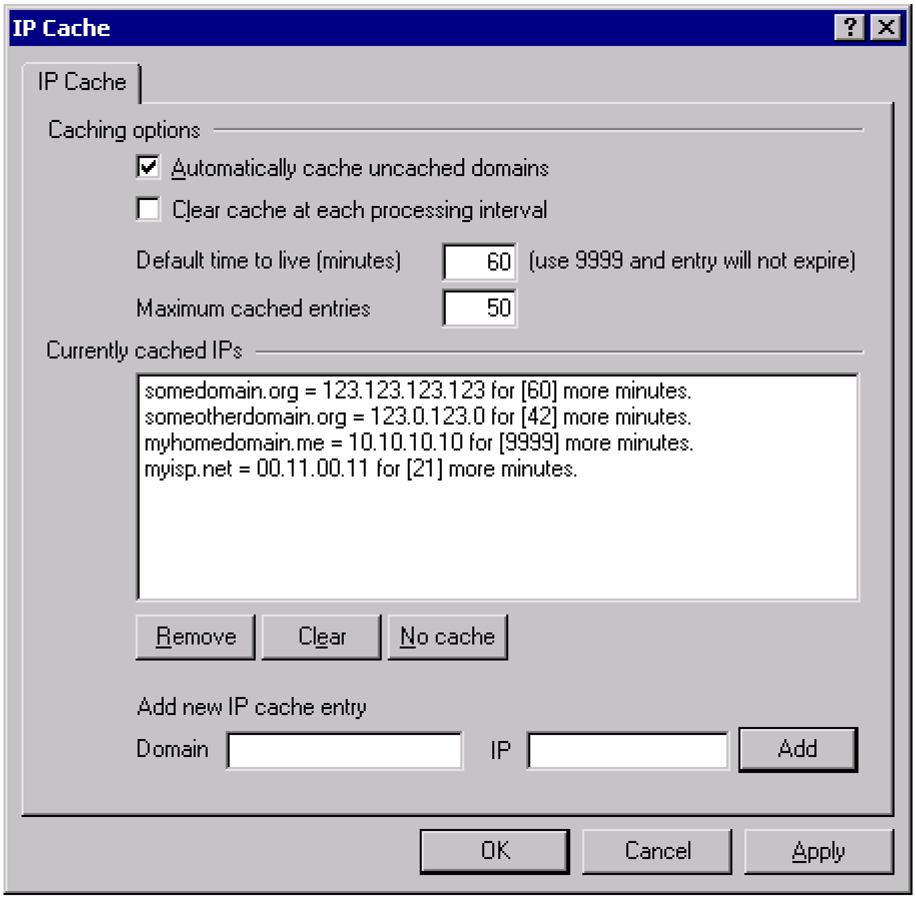
11

IP Cache and DNS Lookup

Using the IP Cache and performing DNS Lookups.

In order to speed message delivery and shorten mail processing time MDaemon caches the IP addresses of all hosts with which it comes in contact. These IP's are stored and the cache is checked each time MDaemon requires a DNS resolution on a domain name. If the domain name needing resolution is found in the IP cache then the DNS lookup is skipped, which can save a surprising amount of processing time. The settings in this window allow you to manipulate the parameters under which the cache will operate. You may also manually add and remove entries and set the maximum size of the cache. The IP Cache can be reached from the **Setup | IP Cache…** menu selection.

IP Cache



Caching options

☑ Automatically cache uncached domains

□ Clear cache at each processing interval

Default time to live (minutes) 60 (use 9999 and entry will not expire)

Maximum cached entries 50

Currently cached IPs

```
somedomain.org = 123.123.123.123 for [60] more minutes.
someotherdomain.org = 123.0.123.0 for [42] more minutes.
myhomedomain.me = 10.10.10.10 for [9999] more minutes.
myisp.net = 00.11.00.11 for [21] more minutes.
```

Add new IP cache entry

Domain ______ IP ______

Caching Options

Clear cache at each processing interval
If selected, the entire contents of the cache will be flushed at the start of each mail session. This allows the cache to be refreshed at each processing interval.

Automatically cache uncached domains
This switch governs **MDaemon's** internal auto-caching engine. If you want MDaemon to cache domains automatically then enable this option. If you want to build the IP Cache yourself, then clear this checkbox.

Default time to live
This is the default value in minutes that an entry in the IP Cache can survive. Once the entry has been in the IP Cache for this number of minutes, MDaemon will remove it. If you want to set a permanent entry in the IP Cache then designate the *Default Time To Live* as 9999 in which case the entry will never expire.

Max cached entries
This value determines how large the cache may be. Once this setting has been reached, the next cache entry will bump the first one out of the cache.

Currently Cached IPs

Remove
Select an entry in the *Currently Cached IPs* window and then click this button to remove it.

No cache
Click this button to bring up a list of domain names and/or IP addresses that you never want MDaemon to add to the IP Cache.

Clear
This button will flush the cache.

Add New IP Cache Entry

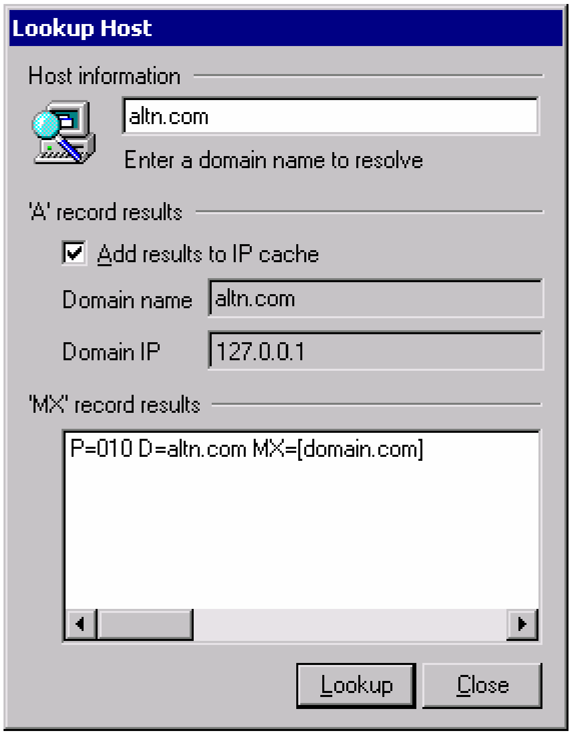
Domain
Enter the domain name that you wish to add to the IP cache.

IP
Enter the IP address that you wish to add to the IP cache.

Add
Once you have entered a domain name and IP address, click this button to manually add them to the cache.

DNS Lookup

The DNS Lookup utility (**Setup|Perform a DNS Lookup…**) can be very useful when used in conjunction with the IP Cache. DNS Lookup makes it possible for you to quickly and easily perform a DNS lookup for any valid Internet domain name. A successfully resolved domain name lookup will display the domain's A-Record and any MX-Records that might be listed. There is also a control that can be used to automatically add the results of a successful lookup to the IP Cache.



Host information

altn.com

Enter a domain name to resolve

'A' record results

☑ Add results to IP cache

Domain name: altn.com

Domain IP: 127.0.0.1

'MX' record results

P=010 D=altn.com MX=[domain.com]

Host Information

Enter the domain name whose DNS information you wish to retrieve.

"A" Record Results

Add results to IP cache
Click this checkbox if you want the results of DNS lookups to be added to the IP Cache.

Domain name
This is the name of the resolved domain name.

Domain IP
This is the resolved domain's IP address.

"MX" Record Results

This window will display any MX records listed for the resolved domain.

Lookup!
Click this button to perform a DNS lookup for the domain name that you have listed in the Host Information section.

Chapter
12

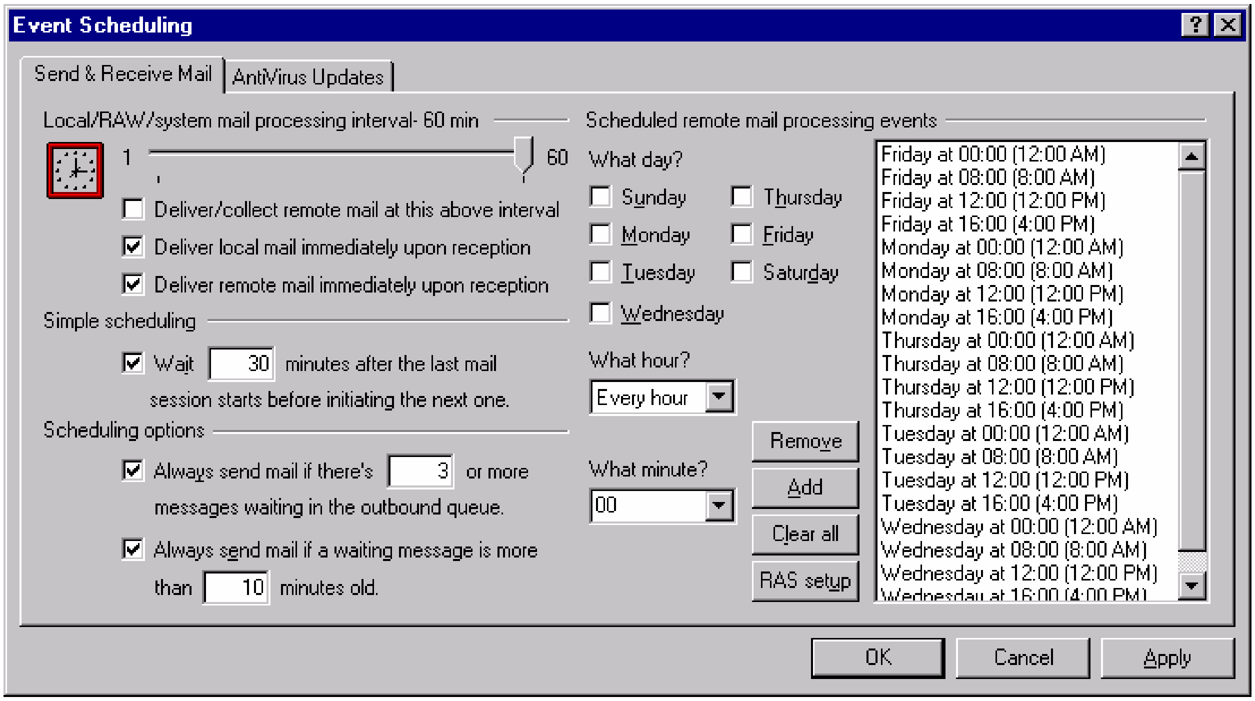
Scheduling and Dialup

Using the Event Scheduler and RAS Dialup/Dialdown Engine.

Click the **Setup→Event scheduling…** menu selection to open MDaemon's Event Scheduler. This dialog makes it possible for you to schedule MDaemon's Local, Remote, RAW, and System mail processing events as extensively or as simply as you prefer. You can schedule exact times for mail delivery and collection or use a counter to process mail at regular intervals. You can also set conditions that will trigger mail processing at unscheduled times such as when a certain number of messages are waiting to be delivered, or when a message has been waiting a specified amount of time. If you have installed MDaemon AntiVirus there will be an additional tab on this dialog called AntiVirus Updates. This tab is used for scheduling how often you want MDaemon AntiVirus to check for virus signature updates.

Event Scheduler

Send & Receive Mail



Local/RAW/system mail processing interval- 60 min

1 — 60

☐ Deliver/collect remote mail at this above interval

☑ Deliver local mail immediately upon reception

☑ Deliver remote mail immediately upon reception

Simple scheduling

☑ Wait 30 minutes after the last mail session starts before initiating the next one.

Scheduling options

☑ Always send mail if there's 3 or more messages waiting in the outbound queue.

☑ Always send mail if a waiting message is more than 10 minutes old.

Scheduled remote mail processing events

What day?

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

What hour? Every hour

What minute? 00

Friday at 00:00 (12:00 AM)
Friday at 08:00 (8:00 AM)
Friday at 12:00 (12:00 PM)
Friday at 16:00 (4:00 PM)
Monday at 00:00 (12:00 AM)
Monday at 08:00 (8:00 AM)
Monday at 12:00 (12:00 PM)
Monday at 16:00 (4:00 PM)
Thursday at 00:00 (12:00 AM)
Thursday at 08:00 (8:00 AM)
Thursday at 12:00 (12:00 PM)
Thursday at 16:00 (4:00 PM)
Tuesday at 00:00 (12:00 AM)
Tuesday at 08:00 (8:00 AM)
Tuesday at 12:00 (12:00 PM)
Tuesday at 16:00 (4:00 PM)
Wednesday at 00:00 (12:00 AM)
Wednesday at 08:00 (8:00 AM)
Wednesday at 12:00 (12:00 PM)
Wednesday at 16:00 (4:00 PM)

Local/RAW/System Mail Processing Interval

Slide this bar left or right to specify the time interval between mail processing sessions. It can be configured to count down from a range of 1 to 60 minutes, after which time MDaemon will *Process Local, RAW, and System Mail* before beginning the countdown again. By default, this gauge only applies to *Local, RAW, and System Mail.* However, by checking the *Deliver remote mail at this interval also* control it will apply to *Remote Mail* as well. When this checkbox is cleared, *Remote Mail* processing intervals will be determined by the other scheduling controls on the *Event Scheduler.*

Deliver/collect remote mail at the above interval

If this checkbox is selected, the slide bar instead of the Scheduler will determine when *Remote Mail* is sent and/or collected. The rest of the controls in the Scheduler will be "dimmed" and will no longer apply to *Remote Mail* processing.

Deliver local mail immediately upon reception

When this option is selected, any *Local, RAW, or System Mail* will be processed and delivered each time an incoming SMTP session has completed. This has the effect of instantaneous delivery of local messages.

Deliver remote mail immediately upon reception

When this option is selected, remote mail will be processed and delivered immediately each time an SMTP session has completed. This has the effect of instantaneous delivery of remote messages.

Simple Scheduling

There are numerous ways a remote mail session can be triggered in MDaemon. Several of them will be discussed in this section of the manual. The *Simple Scheduling* feature is handy when you wish to setup a remote mail processing interval that should occur at a regular time interval after the last one regardless of the trigger that initiates the session. Unlike the rigidly fixed intervals used when setting up specific times or using the slide bar, this feature's time interval will reset whenever mail is processed regardless of what caused the mail session to be initiated.

Note

In order for *Simple Scheduling* to take effect for a given day at least one timed entry must exist for that day in the *Scheduled Times* list. For example, suppose you wanted to schedule 45 minutes between dialup sessions but only on Monday through Friday. You would need to enable the *Simple Scheduling* option and enter 45 minutes into the control and then enter at least one scheduled time for each day (Monday, Tuesday, Wednesday, Thursday, and Friday). Since there would be no scheduled time for Saturday or Sunday, those days would be exempt and would not trigger a *Remote Mail* session. The hour and minute setting you designate when you setup your trigger days doesn't matter; *Simple Scheduling* only checks whether there is an entry present for that day.

Scheduling Options

Always send mail if there's xx or more messages waiting in the outbound queue
MDaemon will trigger a mail session whenever the number of messages waiting in the outbound queue meets or exceeds the number that you specify here. These sessions are in addition to any other normally scheduled sessions.

Always send mail if a waiting message is more than xx minutes old
When this control is enabled, MDaemon will trigger a mail session whenever a message has been waiting in the outbound queue for the number of minutes specified. These sessions are in addition to any other normally scheduled sessions.

Scheduled Remote Mail Processing Events

What day?
Select the days that you wish to schedule.

What hour?
Select the hour that you wish to schedule.

What minute?
Select the minute that you wish to schedule.

Add
Once you've selected the day, hour, and minute click this button to add this time to the list of scheduled events.

Remove
Clicking this button will remove an entry that you have selected from the schedule listing.

Clear all
This button removes all entries from the schedule listing.

RAS setup
This button is provided so that you can quickly review or edit your RAS settings.

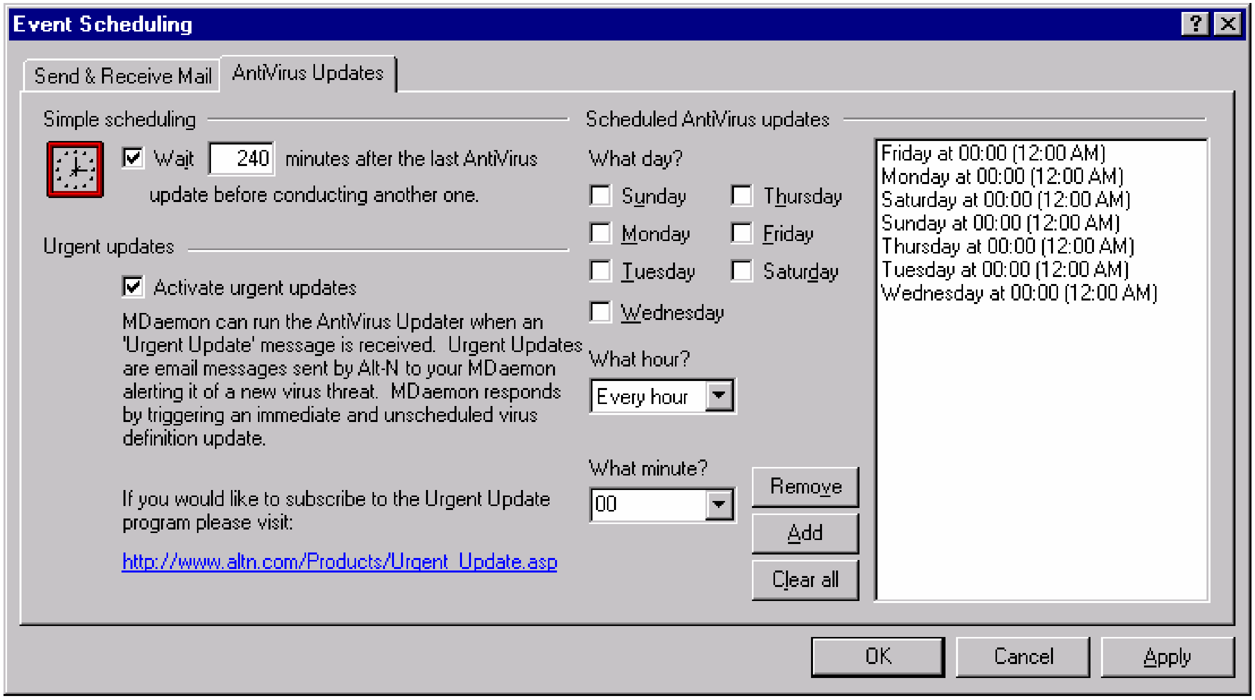
> **Tip**
>
> The amount of time needed to load the Scheduler when MDaemon starts will vary. The length of time this process will take is proportional to the number of event entries that have been created. Most configurations will do well to simply use the slide bar and Simple Scheduling to control mail processing intervals. For example, it is wasteful to schedule every minute of every day using the scheduler when you can simply set the slide bar to one minute intervals, place it in control, and accomplish the same thing. On the other hand, if you want

the remote intervals to be further apart than the local intervals, but still frequent, then you could use *Simple Scheduling* for *Remote* and the slide bar for *Local.*

See:

Configuring Your RAS Settings—page 143

AntiVirus Updates



Event Scheduling

Simple scheduling

☑ Wait 240 minutes after the last AntiVirus update before conducting another one.

Urgent updates

☑ Activate urgent updates

MDaemon can run the AntiVirus Updater when an 'Urgent Update' message is received. Urgent Updates are email messages sent by Alt-N to your MDaemon alerting it of a new virus threat. MDaemon responds by triggering an immediate and unscheduled virus definition update.

If you would like to subscribe to the Urgent Update program please visit:

http://www.altn.com/Products/Urgent_Update.asp

Scheduled AntiVirus updates

What day?

□ Sunday □ Thursday
□ Monday □ Friday
□ Tuesday □ Saturday
□ Wednesday

What hour? Every hour

What minute? 00

Friday at 00:00 (12:00 AM)
Monday at 00:00 (12:00 AM)
Saturday at 00:00 (12:00 AM)
Sunday at 00:00 (12:00 AM)
Thursday at 00:00 (12:00 AM)
Tuesday at 00:00 (12:00 AM)
Wednesday at 00:00 (12:00 AM)

Simple Scheduling

Wait XX minutes after the last AntiVirus update before conducting another one.

Click this checkbox and specify the number of minutes that you want MDaemon AntiVirus to wait before checking for new virus signature updates. Note, this is actually the number of minutes that MDaemon AntiVirus will *attempt* to wait after the last time you checked for an update, whether the update was triggered by the scheduler or manually. The scheduler and manually triggered updates are given precedence over Simple Scheduling and it will therefore reset this counter if an AntiVirus Update event is triggered by one of those other methods. Thus, for example, if you have this option set to check for updates every 240 minutes and you manually check for an update after 100 minutes have passed then this counter start over again at 240.

Urgent Updates

Activate urgent updates

Click this checkbox to activate the urgent updates feature. With this feature enabled, MDaemon AntiVirus will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message. To receive these messages you must first subscribe to the “Urgent Updates” mailing list at “`http://www.altn.com/Products/Urgent_Update.asp`”. See AntiVirus Updater (page 180) for more information.

Scheduled AntiVirus Updates

What day?
Select the days that you wish to schedule.

What hour?
Select the hour that you wish to schedule.

What minute?
Select the minute that you wish to schedule.

Add
Once you’ve selected the day, hour, and minute click this button to add this time to the list of scheduled events.

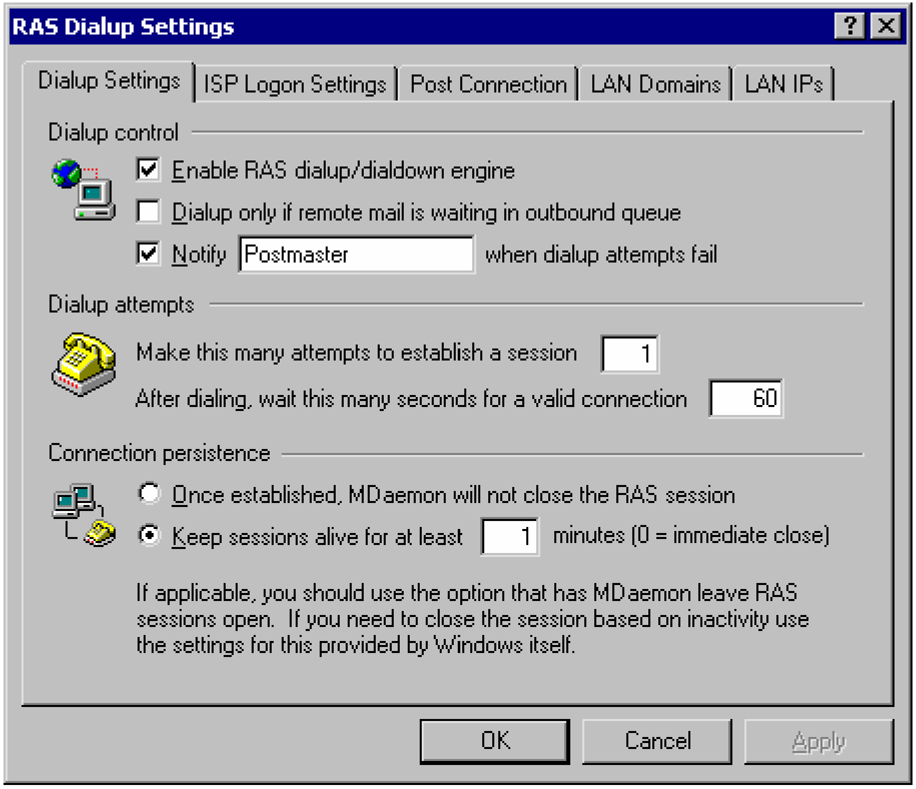
Remove
Clicking this button will remove an entry that you have selected from the schedule listing.

Clear all
This button removes all entries from the schedule listing.

RAS Dialup Settings

Click the **Setup|RAS Dialup/Dialdown…** menu selection to configure your RAS Dialup Settings. This dialog will only be available if you have Remote Access Services installed on your system. It is used by MDaemon when you need to dial up your ISP just prior to a Remote Mail processing event.

Dialup Settings



Dialup control

☑ Enable RAS dialup/dialdown engine

□ Dialup only if remote mail is waiting in outbound queue

☑ Notify Postmaster when dialup attempts fail

Dialup attempts

Make this many attempts to establish a session 1

After dialing, wait this many seconds for a valid connection 60

Connection persistence

○ Once established, MDaemon will not close the RAS session

● Keep sessions alive for at least 1 minutes (0 = immediate close)

If applicable, you should use the option that has MDaemon leave RAS sessions open. If you need to close the session based on inactivity use the settings for this provided by Windows itself.

Dialup Control

Enable RAS dialup/dialdown engine

Selecting this option will cause MDaemon to use the settings specified here to make a connection to a remote host before sending and/or receiving remote mail.

Dialup only if remote mail is waiting in outbound queue

When this switch is checked, MDaemon will not dial up the ISP unless there is remote mail waiting in the Remote queue. This may be beneficial in some circumstances but be aware that if MDaemon does not dial up then it cannot do any mail **collecting** either (unless it is delivered across the local LAN).

Notify [address] when dialup attempts fail

When selected, MDaemon will send a message to the specified address when a dialup event fails because of some error.

Dialup Attempts

Make this many attempts to establish a session

MDaemon will attempt to connect to the remote host this many times before giving up.

After dialing, wait this many seconds for a valid connection

This value determines how long MDaemon will wait for the remote computer to answer and complete the RAS connection.

Connection Persistence

Once established, MDaemon will not close the RAS session

By default, MDaemon will shut down a created connection immediately after all mail transactions have been completed, and the session is no longer in use. Selecting this option will cause the connection to remain open even after all transactions have been completed.

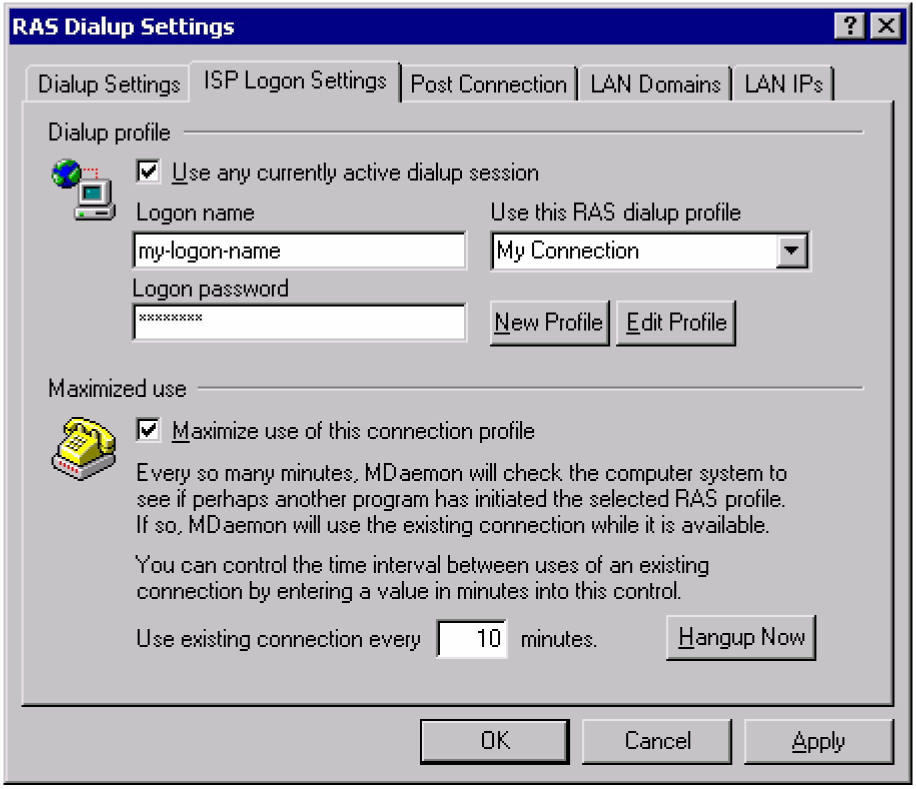
Note

MDaemon will never close a connection that it did not create.

Keep sessions alive for at least xx minutes

If enabled, this option will cause an MDaemon created RAS session to remain open for at least the number of minutes specified or until all mail transactions have been completed, whichever is greater.

ISP Logon Settings



☑ Use any currently active dialup session

Logon name: my-logon-name

Use this RAS dialup profile: My Connection

Logon password: ********

☑ Maximize use of this connection profile

Every so many minutes, MDaemon will check the computer system to see if perhaps another program has initiated the selected RAS profile. If so, MDaemon will use the existing connection while it is available.

You can control the time interval between uses of an existing connection by entering a value in minutes into this control.

Use existing connection every 10 minutes.

Dialup Profile

Use any currently active dialup session
Click this checkbox if you want MDaemon to be able to utilize other connection profiles when it detects that one is active. Whenever it is time to dialup, MDaemon will first check to see if there is an active connection that it can use rather than dialing.

Logon name
The value specified here will be passed to the remote host during the authentication process.

Logon Password
The value specified here will be passed to the remote host during the authentication process.

Use this RAS dialup profile
This drop-down list box allows you to select a session profile that has been previously defined through windows Dialup Networking or Remote Access Services Setup.

New profile
Click this button to create a new Dialup Networking or Remote Access Services profile.

Edit profile
Click this button to edit the currently selected Dialup Networking or Remote Access Services profile.

Maximized Use

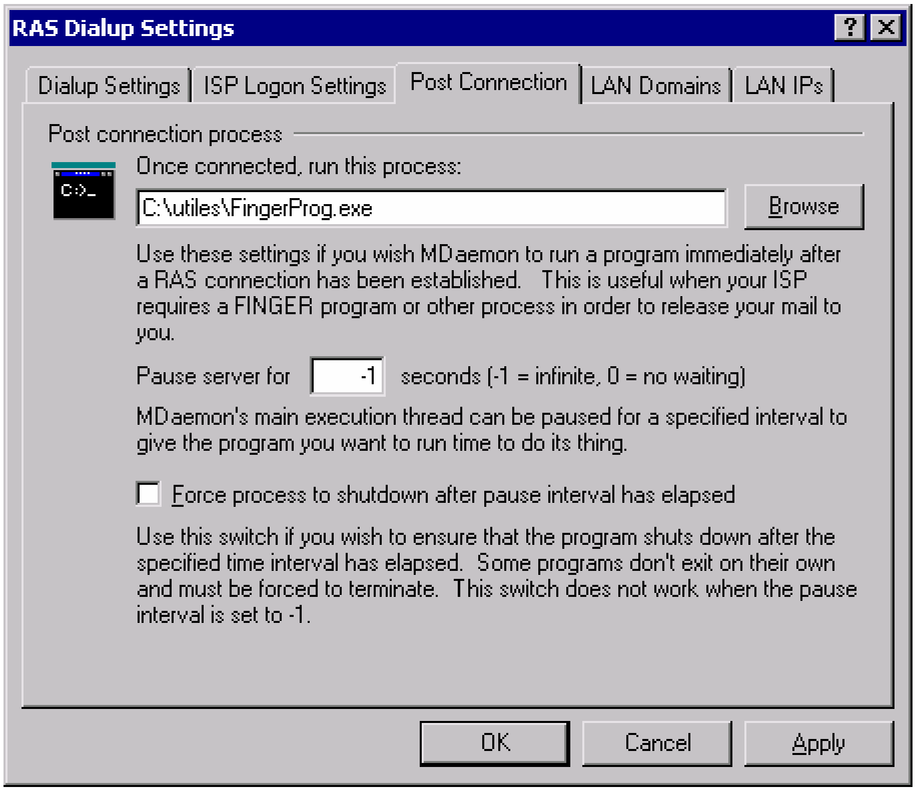
Maximize use of this connection profile

This switch causes MDaemon to monitor your connections so that if it detects that another program has established a connection it will process remote mail immediately regardless of scheduled times. If the connection remains open it will continue to process remote mail at regular time intervals based on the *Use existing connection every XX minutes* setting.

Hang-up now

This button will close the connection to the ISP. This button is active only if MDaemon has initiated the RAS session.

Post Connection



Post connection process

Once connected, run this process:

C:\utiles\FingerProg.exe

Use these settings if you wish MDaemon to run a program immediately after a RAS connection has been established. This is useful when your ISP requires a FINGER program or other process in order to release your mail to you.

Pause server for -1 seconds (-1 = infinite, 0 = no waiting)

MDaemon's main execution thread can be paused for a specified interval to give the program you want to run time to do its thing.

□ Force process to shutdown after pause interval has elapsed

Use this switch if you wish to ensure that the program shuts down after the specified time interval has elapsed. Some programs don't exit on their own and must be forced to terminate. This switch does not work when the pause interval is set to -1.

Post Connection Process

Once connected, run this process

If a program is specified here, MDaemon will spawn a thread and execute the process. This is extremely useful for those who require `Finger` or some other program to unlock the ISP's mailbox.

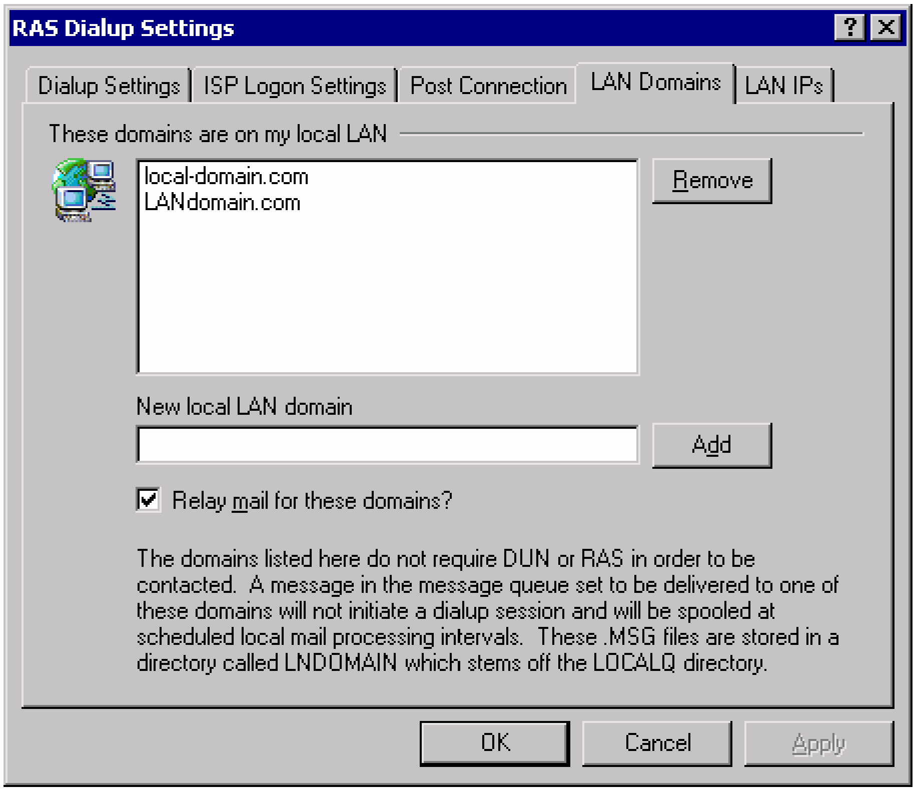
Pause server for xx seconds (-1 = infinite, 0=no waiting)

If the *Once Connected, Run This Process* control contains a valid entry then the server will pause its operations for the number of minutes specified here while it waits for the executing process to return. Entering "-1" will cause the server to wait indefinitely for the process to return.

Force process to shutdown after pause interval has elapsed

Sometimes the program you need to run may not exit once it has run its course; some programs require user intervention in order to close them down. This is not acceptable when the software must run unattended. If this switch is selected MDaemon will force the process thread to terminate once the number of seconds specified in *Pause Server For XX Seconds* has elapsed. This function does not work when the server is configured to wait indefinitely for the process to return.

LAN Domains



These domains are on my local LAN

local-domain.com
LANdomain.com

New local LAN domain

☑ Relay mail for these domains?

The domains listed here do not require DUN or RAS in order to be contacted. A message in the message queue set to be delivered to one of these domains will not initiate a dialup session and will be spooled at scheduled local mail processing intervals. These .MSG files are stored in a directory called LNDOMAIN which stems off the LOCALQ directory.

These domains are on my local LAN

The domains listed here are considered by MDaemon to be part of your local LAN. Therefore, no dialup is required in order to deliver a message to one of them.

New local LAN domain

Enter a domain name to add to the Local LAN list and click the *Add* button to add it.

Relay mail for these domains

If this switch is selected MDaemon will relay mail for these domains. This provides some measure of control over the traffic sent to and from these domains.

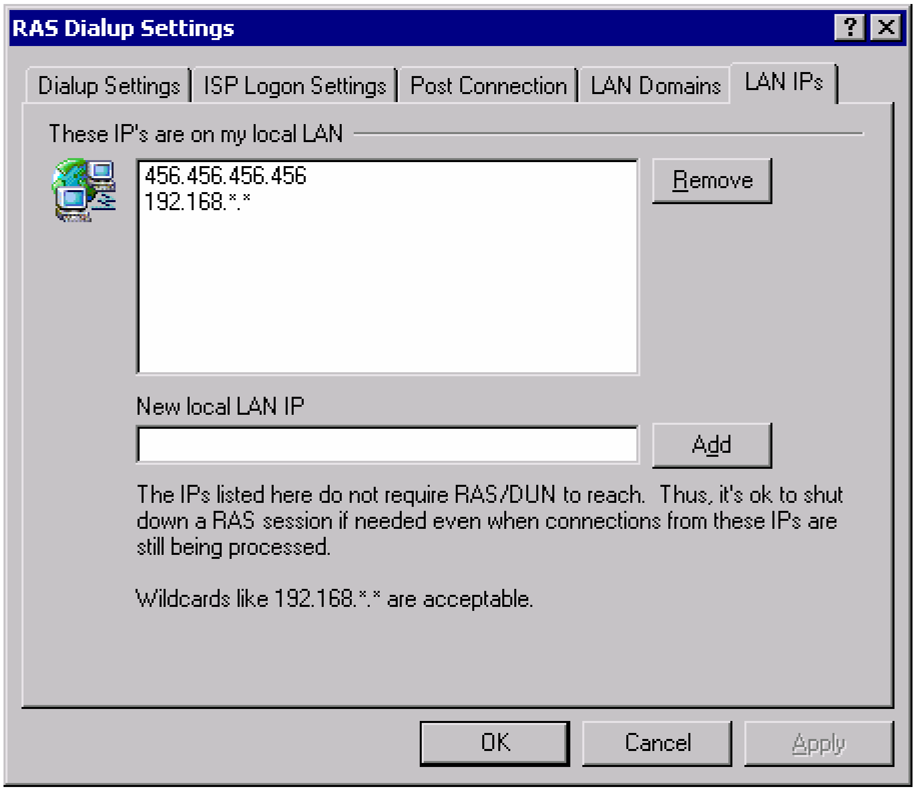
Add

Click this button to add an entry to the list of LAN domains.

Remove

Click this button to remove a selected entry from the list of LAN Domains.

LAN IPs



These IP's are on my local LAN

456.456.456.456
192.168.*.*

New local LAN IP

The IPs listed here do not require RAS/DUN to reach. Thus, it's ok to shut down a RAS session if needed even when connections from these IPs are still being processed.

Wildcards like 192.168.*.* are acceptable.

These IPs are on my local LAN

Like the LAN Domains tab, this tab is used to list IP addresses that reside on your LAN and thus do not require dialup in order to deliver messages to them. If a RAS session is in progress while messages are being delivered to these IP addresses and no non-local addresses remain, MDaemon will close the RAS session and continue to deliver the remaining Local IP messages.

Remove

Select an IP address from the list and then click this button to remove it. You may also double click an entry to remove it.

New local LAN IP

Enter an IP address to add to the local IP list and click *Add*. Wildcards like 127.0.*.* are permitted.

Add

After entering an IP Address into the *New local LAN IP* control, click this button to it to the list.

Chapter

13

DomainPOP Mail Collection

Using MDaemon's DomainPOP Mail Collection features.

Use DomainPOP Mail Collection (**Setup|DomainPOP Mail Collection…**) to configure MDaemon to download mail from a remote POP mailbox for redistribution to your users. This feature works by using the POP protocol to download all the mail found in the ISP's POP mailbox associated with the specified logon. Once collected, the messages are parsed according to the settings provided on this dialog and then placed in user mailboxes or the remote mail queue for MDaemon to deliver, just as if the messages had arrived at the server using conventional SMTP transactions.

It is important to note that messages stored in POP mailboxes and retrieved using the POP protocol will be devoid of the important routing information (sometimes called the message's "envelope") that would ordinarily be supplied had the messages been delivered using the more powerful SMTP protocol. Without this routing information, MDaemon is forced to "read" the message and examine the headers in an attempt to determine to whom the message was originally intended. This is not an exact science to say the least. Message headers are sometimes notorious for their lack of sufficient information that is needed to determine the intended recipient. This lack of what would seem to be a fundamental characteristic of an email message - the recipient - may seem surprising but one must keep in mind that the message was never intended to be delivered to its recipient using the POP protocol. With SMTP, the contents of the message are irrelevant since the protocol itself dictates specifically to the server, during the mail transaction, the intended recipient of the message.

In order to allow for POP retrieval and delivery of mail messages in a reliable and consistent way, MDaemon employs a powerful suite of header processing options. When MDaemon downloads a message from a remote POP source it immediately parses all the relevant headers within that message and builds a collection of potential recipients. Every email address found in the headers that MDaemon inspects is included in the collection.

Once this process is complete, MDaemon's collection of recipients is divided into local and remote sets. Further, all addresses that are parsed and placed into the collection of potential recipients are processed through the Address Alias translator before being divided into local and remote sets. Every member of the local set (addresses with a domain that matches either MDaemon's Primary domain or one of the Secondary domains) will receive a copy of the message. What happens to the remote set is governed by the settings in this dialog. You can elect to simply ignore these addresses, forward a summary listing of them to the postmaster, or honor them—in which case MDaemon will actually deliver a copy of the message to the remote recipient. Only under rare circumstances would the need to deliver these messages to remote recipients be warranted.

Care must be taken to prevent duplicate messages or endlessly looping mail delivery cycles. A common problem that results from the loss of the SMTP envelope manifests itself with mailing list mail. Typically, messages distributed by a mailing list do not contain within the message body any reference to the addresses of the recipients. Rather, the list engine simply inserts the name of the mailing list into the `TO:` field. This presents an immediate problem: if the `TO:` field contains the name of the mailing list then the potential exists for MDaemon to download this message, parse the `TO:` field (which will yield the name of the mailing list), and then dispatch the message right back to the same list. This would in turn deliver another copy of the same message back to the POP mailbox from which MDaemon downloaded the original message—thus starting the whole cycle over again. To cope with such problems mail administrators must take care to use the tools and settings that MDaemon provides to either delete mailing list mail or perhaps alias it in such a way that it will be delivered to the proper local recipient(s). You could also utilize the Routing Rules or Content Filters to deliver the message to the correct recipient(s).

Additional concerns when employing this sort of mail collection scheme revolve around the issue of unwanted message duplication. It is very easy for mail that is delivered to the ISP's POP mailbox using SMTP to generate unwanted duplicates, once it has been collected using DomainPOP. For example, suppose a message is sent to someone at your domain and a carbon copy is sent to another person at the same domain. In this situation, SMTP will deliver **two** copies of the same message to your ISP's mailbox—one for each recipient. Each of the two message files will contain references to **both** recipients—one in the `TO:` field and the other in the `CC:` field. MDaemon will collect each of these two identical message files and parse both addresses from each of them. This would result in both recipients receiving one unwanted duplicate message. To guard against this sort of duplication MDaemon uses a control which allows you to specify a header that MDaemon will use to check for duplication. The `Message-ID` field is ideal for this. In the above example, both messages are identical and will therefore contain the same `Message-ID` field value. MDaemon can use this value to identify and remove the second message during the download stage before it can be parsed for address information.

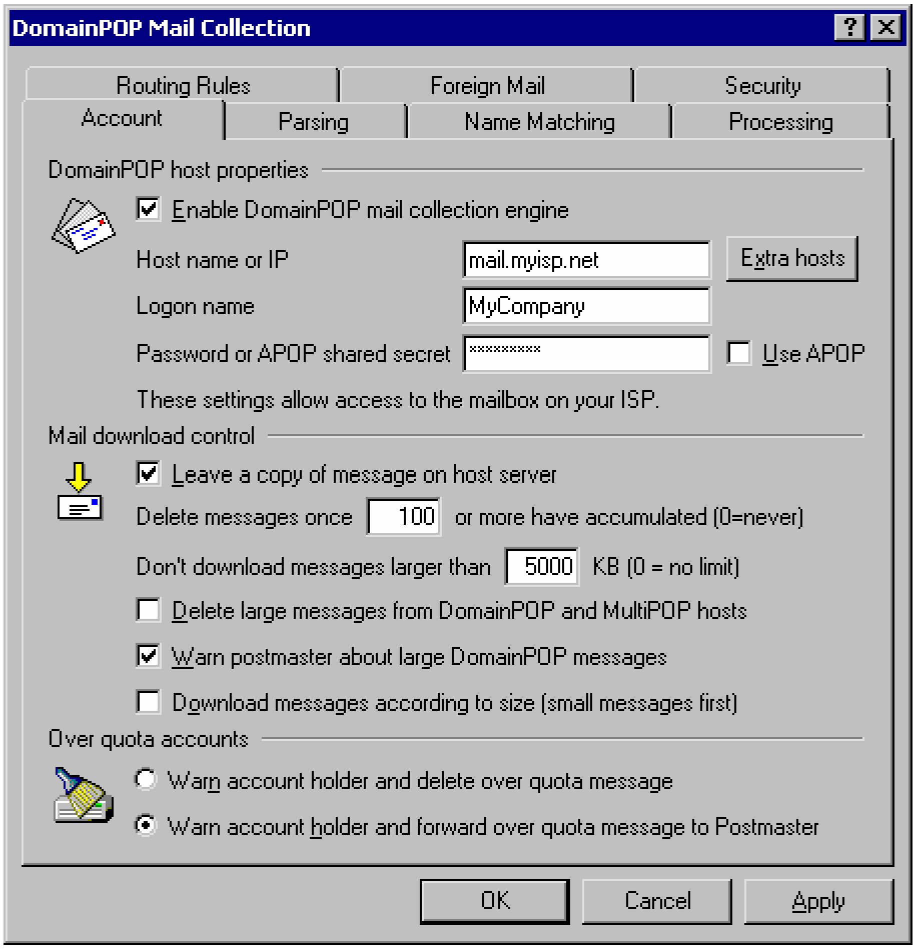
As a final measure guarding against duplicate messages and endless looping delivery cycles, MDaemon employs a means for detecting how many trips or "hops" a message has made through the transport system. Each time an SMTP mail server processes a message it "stamps" the message with a "Received" header. MDaemon counts all such headers when it encounters a message for the first time. If the total number of mail servers exceeds a specified value, it is likely the message is caught in a delivery loop and should be taken out of the mailstream and moved to the bad message directory. This value can be configured through the Domain Configuration Editor (page 45).

See:

Primary Domain Configuration—page 34
Content Filters—page 166
Mailing Lists—page 268

DomainPOP Mail Collection

Account



DomainPOP host properties

☑ Enable DomainPOP mail collection engine

Host name or IP: mail.myisp.net

Logon name: MyCompany

Password or APOP shared secret: ********* □ Use APOP

These settings allow access to the mailbox on your ISP.

Mail download control

☑ Leave a copy of message on host server

Delete messages once 100 or more have accumulated (0=never)

Don't download messages larger than 5000 KB (0 = no limit)

□ Delete large messages from DomainPOP and MultiPOP hosts

☑ Warn postmaster about large DomainPOP messages

□ Download messages according to size (small messages first)

Over quota accounts

○ Warn account holder and delete over quota message

● Warn account holder and forward over quota message to Postmaster

DomainPOP Host Properties

Enable DomainPOP mail collection engine

If selected, MDaemon will use the setting provided on this screen to collect mail from a DomainPOP mail host for local redistribution.

Host name or IP

Enter your DomainPOP host's domain name here. Additionally, if you wish to specify a port to collect the mail from other than MDaemon's current default POP port, you can do so by appending a new port value to the host name separated by a colon. For example, using "`mail.altn.com`" as a DomainPOP host will connect to that host using the default outbound POP port while using "`mail.altn.com:523`" will connect to that host on port 523.

Logon name

Enter your logon of the POP account used by DomainPOP.

Password or APOP shared secret

Enter the POP account's password or APOP shared secret here.

Use APOP

Click this box if you wish to use the APOP command and CRAM-MD5 authentication when retrieving your mail. This makes it possible to authenticate yourself without having to send clear text passwords.

Mail Download Control

Leave a copy of message on host server

If selected, MDaemon will not remove collected messages from your DomainPOP mail host.

Delete messages once [xx] or more have accumulated (0 = no limit)

If you are leaving messages on your ISP server then they will be deleted once this number is reached. Enter "0" if you want messages to remain on the server regardless of the number.

Note

Some ISP's may limit the amount that you are allowed to store in your mailbox.

Don't download messages larger than [xx] KB (0 = no limit)

Messages greater than or equal to this size will not be downloaded from your DomainPOP mail host. Enter "0" if you want MDaemon to download messages no matter the size.

Delete large messages from DomainPOP and MultiPOP hosts

Click this switch and MDaemon will delete messages that exceed your maximum set size. The messages will simply be removed from the DomainPOP and MultiPOP mail hosts and will not be downloaded.

Warn postmaster about large DomainPOP messages

Click this switch and MDaemon will send a warning to the postmaster whenever a large message is discovered in the DomainPOP mailbox.

Download messages according to size (small messages first)

Enable this checkbox if you want the message downloading order to be based on size—beginning with the smallest and proceeding to the largest.

Note

This option retrieves smaller messages quicker but requires a larger amount of internal sorting and processing.

Over Quota Accounts

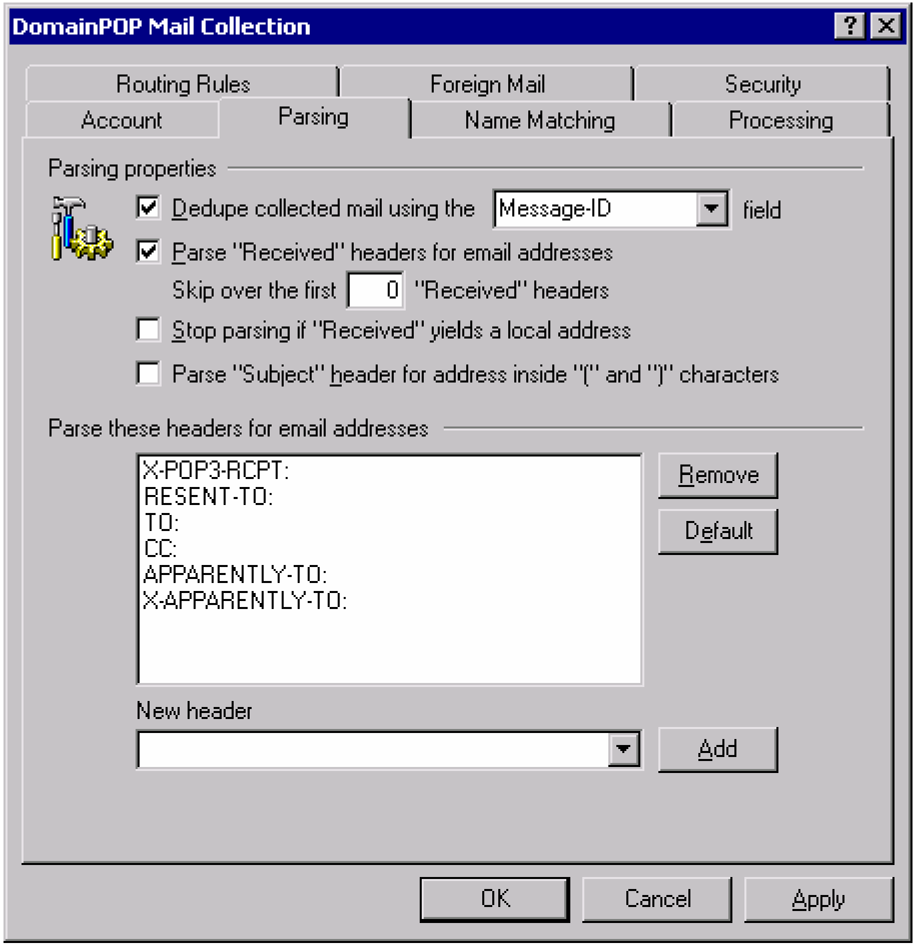
Warn account holder and delete over quota message

When this option is chosen and a message is collected for an account that is over its quota (designated on the Quotas tab of the account editor), MDaemon will delete the message and send a warning to the user letting them know that their account is over its limit.

Warn account holder and forward over quota message to Postmaster

When this option is chosen and a message is collected for an account that is over its quota (designated on the Quotas tab of the account editor), MDaemon will forward the message to the Postmaster and send a warning to the user letting them know that their account is over its limit.

Parsing



Parsing properties

☑ Dedupe collected mail using the Message-ID field

☑ Parse "Received" headers for email addresses

Skip over the first 0 "Received" headers

☐ Stop parsing if "Received" yields a local address

☐ Parse "Subject" header for address inside "(" and ")" characters

Parse these headers for email addresses

```
X-POP3-RCPT:
RESENT-TO:
TO:
CC:
APPARENTLY-TO:
X-APPARENTLY-TO:
```

New header

Parsing Properties

De-dupe collected mail using the Message-ID field

If this option is selected MDaemon will remember the value of the specified header and will not process additional messages collected in the same processing cycle which contain an identical value. The `Message-ID` field is the natural header to use but the actual header can be anything you want.

Parse "Received" headers for email addresses

This switch makes use of a powerful yet seldom used optional RFC-822 regulation. It is possible to store the recipient information ordinarily found only within the message's envelope in a message header so that parsers of the mail message will be able to glean the actual recipient address by merely inspecting the headers later. MDaemon will attempt to capitalize on this optional rule if you have this switch set by parsing ALL the "received" headers found within the mail message for valid addresses.

Skip over the first xx "Received" headers

Sometimes it is useful to process Received headers but starting at the nth occurrence of them. This setting allows you to enter the number of "Received" headers that MD will skip over before beginning its processing.

Stop parsing if "Received" yields a valid local address

If while parsing a "received" header MDaemon detects a valid local address, this switch will cause all further parsing to stop and MDaemon will not search the message for more potential delivery addresses.

Parse "Subject:" header for address inside "(" and ")" characters
When this is selected and MDaemon finds an address contained in "( )" in the "Subject:" header of a message, this address will be added to the message's list of recipients along with any other parsed addresses.

Parse these headers for email addresses

This control lists the headers that MDaemon will parse in an attempt to extract addresses. Every header listed here is checked for addresses.

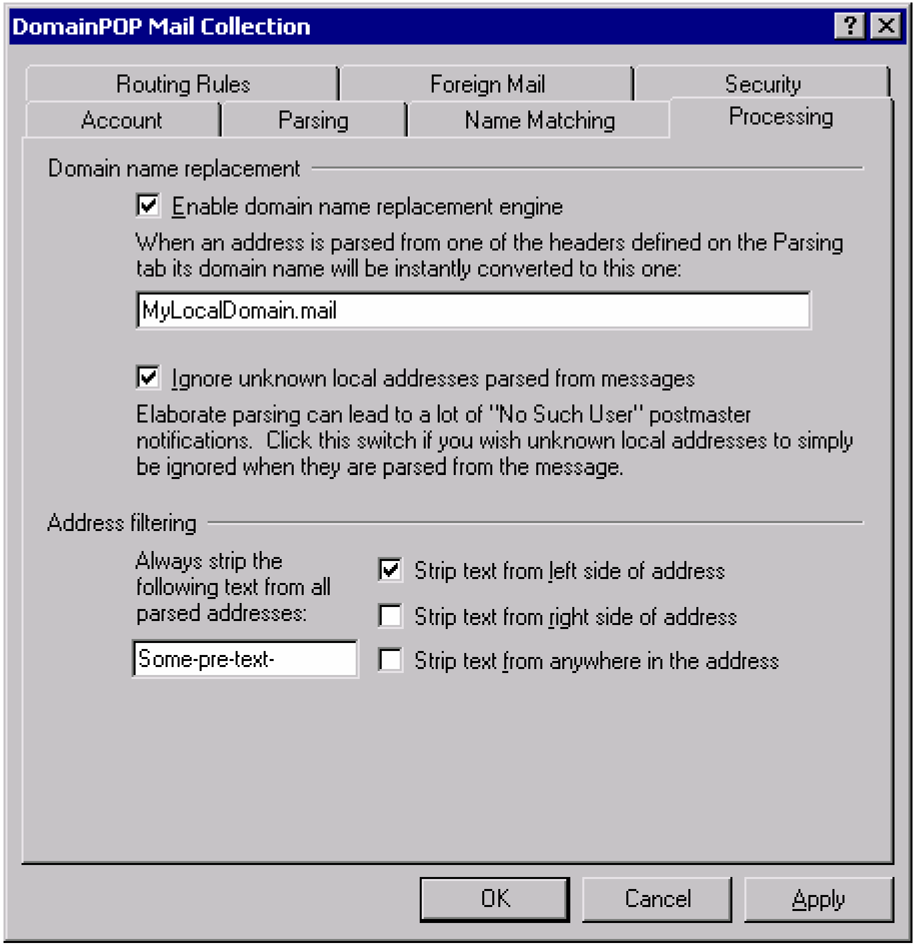
Remove
This button will remove the selected entries from the header list.

Default
This button will clear the current contents of the header list and add MDaemon's default list of headers. The default headers are typically sufficient to extract all addresses from the message.

New header
Enter the header you wish to add to the header list.

Add
Add the header listed in the *New Header* control to the list.

Processing



Domain name replacement

☑ Enable domain name replacement engine

When an address is parsed from one of the headers defined on the Parsing tab its domain name will be instantly converted to this one:

MyLocalDomain.mail

☑ Ignore unknown local addresses parsed from messages

Elaborate parsing can lead to a lot of "No Such User" postmaster notifications. Click this switch if you wish unknown local addresses to simply be ignored when they are parsed from the message.

Address filtering

Always strip the following text from all parsed addresses:

Some-pre-text-

☑ Strip text from left side of address

□ Strip text from right side of address

□ Strip text from anywhere in the address

Domain Name Replacement

Enable domain name replacement engine

This option is an attempt to cut down on the number of domain aliases your site will require. When a message is downloaded *all* domain names in *all* addresses which are parsed from that message are instantly transformed into the one specified here.

Ignore unknown local addresses parsed from messages

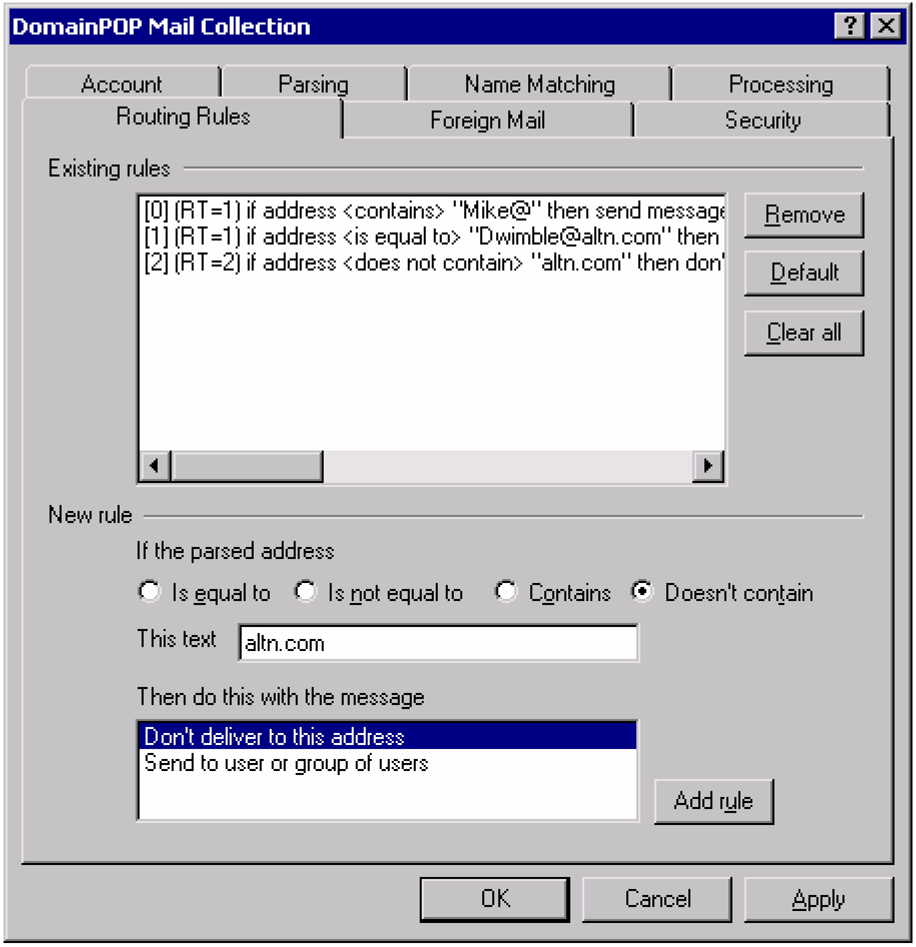
As mentioned above, the Domain Name Replacement feature will alter the domain name in all email addresses parsed from the message, converting it into the one you specify on this screen. This could create some addresses which do not have a corresponding mailbox account at your site. Since the domain name will match your primary domain name, MDaemon will consider such addresses local but undefined. Such mail typically generates a "No Such User" message directed at the postmaster. This switch will prevent the Domain Name Replacement Engine from generating "No Such User" messages.

Address Filtering

Always strip the following text from all parsed addresses

Some ISP's will stamp each message with a line that indicates who the recipient of the message should be along with a bit of routing information appended to the address on either the left or right hand side. This stamp would be perfect to use for parsing the recipient address except that the additional routing information makes this impossible without a lot of account aliasing. Rather than do all that you can simply specify the value of this appended text in the edit control associated with this feature and MDaemon will strip any occurrence of this text from all addresses that it parses.

Routing Rules



Existing rules:

```
[0] (RT=1) if address <contains> "Mike@" then send messag
[1] (RT=1) if address <is equal to> "Dwimble@altn.com" then
[2] (RT=2) if address <does not contain> "altn.com" then don'
```

If the parsed address

○ Is equal to ○ Is not equal to ○ Contains ● Doesn't contain

This text: altn.com

Then do this with the message

- Don't deliver to this address (selected)
- Send to user or group of users

Existing Rules

This list shows you the rules that you have created and will be applied to your messages.

Remove
Press this button and the selected rules in the *Existing Rules* list will be removed.

Default
Press this button to remove all existing rules and replace them with a predefined set of defaults.

Clear all
This button removes all existing rules.

New Rule

If the parsed address…

Is equal to, is not equal to, contains, does not contain
This is the type of comparison that will be made when an address is compared to this routing rule. MDaemon will search each address for the text contained in the "*This text*" field and then proceed based

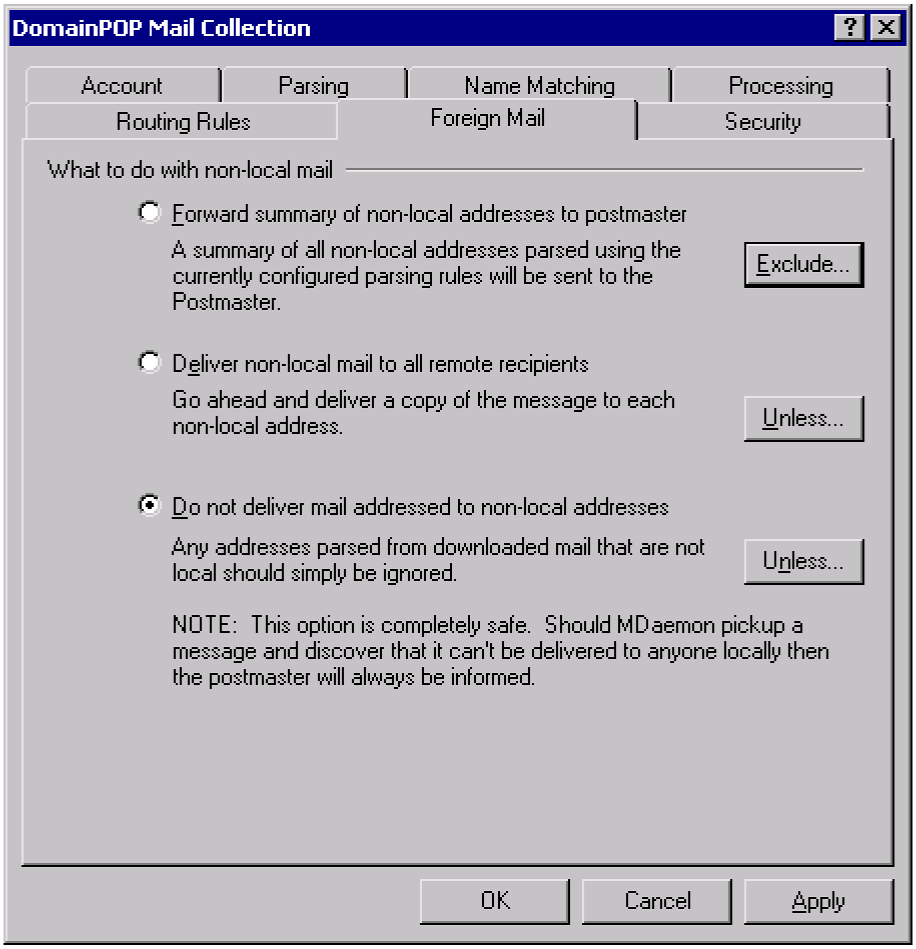
upon this control's setting—does the address's complete text match exactly, not match exactly, contain the text, or not contain it at all?

This text
Enter the text that you want MDaemon to search for when scanning the addresses.

Then do this with the message
This control lists the available actions that can be performed if the result of the rule is true. Here is a list of actions and what they do:

> ***Don't deliver to this address -*** Selecting this rule will prevent the message from being delivered to the specified address.
>
> ***Send to user or group of users*** - Selecting this action will bring up a dialog that will allow you to create a list of email addresses that should receive a copy of the message being processed.

Foreign Mail



What to do with non-local mail

○ Forward summary of non-local addresses to postmaster

A summary of all non-local addresses parsed using the currently configured parsing rules will be sent to the Postmaster.

○ Deliver non-local mail to all remote recipients

Go ahead and deliver a copy of the message to each non-local address.

● Do not deliver mail addressed to non-local addresses

Any addresses parsed from downloaded mail that are not local should simply be ignored.

NOTE: This option is completely safe. Should MDaemon pickup a message and discover that it can't be delivered to anyone locally then the postmaster will always be informed.

What to do with non-local mail

Forward summary of non-local addresses to postmaster

If this option is selected MDaemon will send a single copy of the message to the postmaster along with a summary of the non-local addresses that the parsing engine extracted using the current set of headers and parsing rules.

Deliver non-local mail to all remote recipients

If this option is selected MDaemon will deliver a copy of the message to any non-local recipient that it finds within the inspected headers.

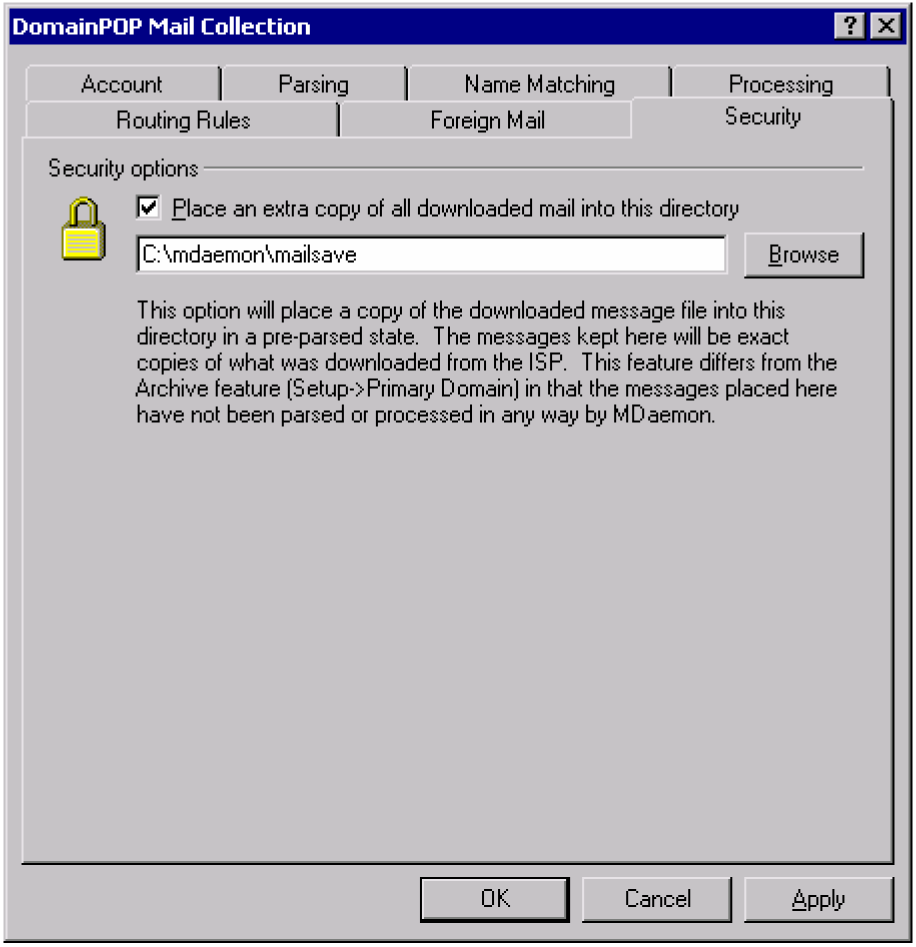
Do not deliver mail addressed to non-local addresses

If this option is selected MDaemon will remove from the recipient list any address that is non-local. It will be as if MDaemon never parsed remote addresses from the original downloaded message.

Note

The various *Unless..* buttons allow you to define addresses which are exceptions to the rules.

Security



Security options

☑ Place an extra copy of all downloaded mail into this directory

C:\mdaemon\mailsave

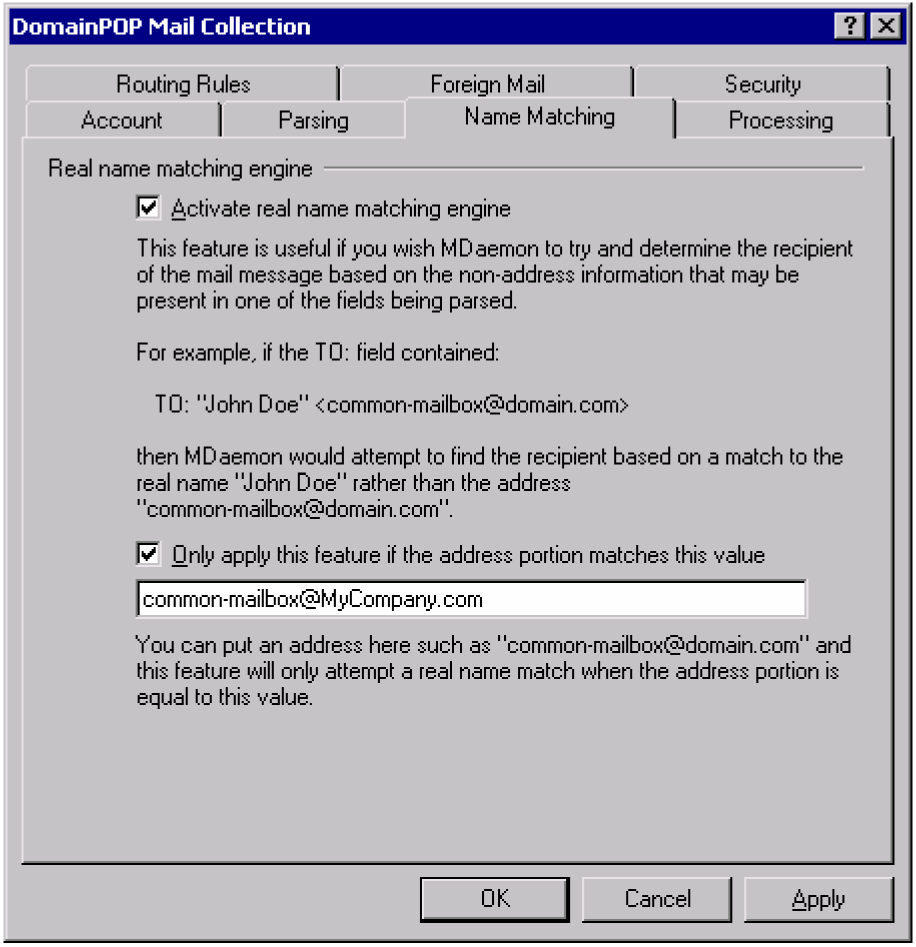
This option will place a copy of the downloaded message file into this directory in a pre-parsed state. The messages kept here will be exact copies of what was downloaded from the ISP. This feature differs from the Archive feature (Setup->Primary Domain) in that the messages placed here have not been parsed or processed in any way by MDaemon.

Safety Options

Place an extra copy of all downloaded mail into this directory

This is a safety feature to ensure that you don't lose any mail due to unforeseen parsing or other errors that might occur when downloading mail in bulk quantities.

Name Matching



Real name matching engine

☑ Activate real name matching engine

This feature is useful if you wish MDaemon to try and determine the recipient of the mail message based on the non-address information that may be present in one of the fields being parsed.

For example, if the TO: field contained:

TO: "John Doe" <common-mailbox@domain.com>

then MDaemon would attempt to find the recipient based on a match to the real name "John Doe" rather than the address "common-mailbox@domain.com".

☑ Only apply this feature if the address portion matches this value

common-mailbox@MyCompany.com

You can put an address here such as "common-mailbox@domain.com" and this feature will only attempt a real name match when the address portion is equal to this value.

Note

The Name Matching feature is only active in conjunction with the DomainPOP Mail Collection engine. If you wish to use this feature, you must make sure that you have DomainPOP enabled. DomainPOP can be reached from the **Setup|DomainPOP Mail Collection** menu selection.

Real Name Matching Engine

Activate real name matching engine

This feature allows MDaemon to determine who should receive a DomainPOP collected message based not upon what the email address is but upon what the text portion (typically a person's real name) is. For example, a message's TO header might read:

```
TO: "Joe User" <common-mailbox@isp.com>
```

or

```
TO: Joe User <common-mailbox@isp.com>
```

Name Matching does not care about the "common-mailbox@isp.com" portion of the address. It instead extracts the "Joe User" portion and attempts to lookup this name in the MDaemon user database. If a match is found to an account's real name field then that account's local email address is used for delivery purposes. If no match is made then MDaemon reverts to delivering the message to the email address parsed from the data (common-mailbox@isp.com in this example).

Note

The real name portion of the address should not contain a comma, semi-colon, or colon character so take care when you setup this information in your mail clients.

Only apply this feature if the address portion matches this value

This control allows you to specify an email address that must be present in the extracted data in order for the real name matching process to proceed. This allows you a measure of control over when the Name Matching feature will be employed. For example, you can specify an address such as "common-mailbox@isp.com" and then only addresses matching this value will be candidates for Name Matching.

Suppose you have "common-mailbox@isp.com" in this control.

This means that:

`TO: "Joe User" <common-mailbox@isp.com>` will be a candidate for Name Matching while **`TO: "Joe User" <Joe@mdaemon.com>`** will not.

Chapter

14

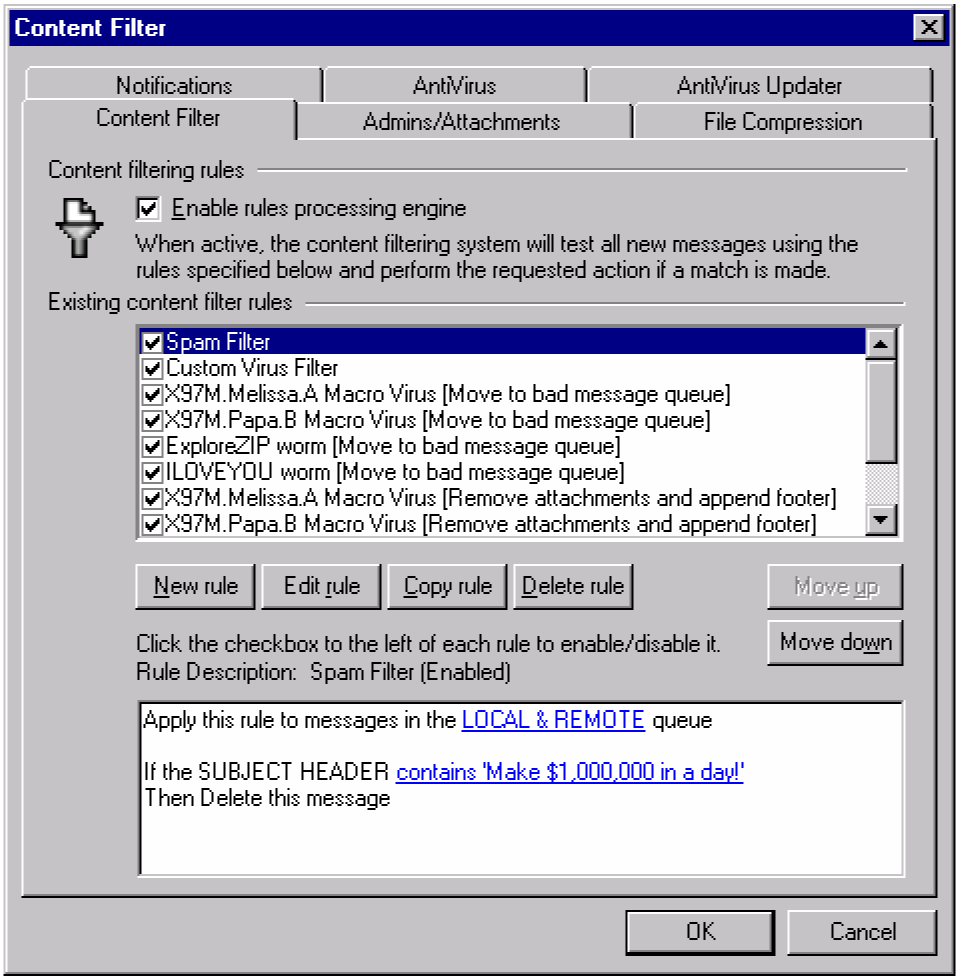
Content Filter and Anti-virus

Filtering messages and scanning for viruses.

The Content Filter dialog (**Setup→Content Filter…**) can be used for a large number of purposes such as: preventing spam email, intercepting messages containing viruses before they reach their final destination, copying certain emails to one or more additional users, appending a note or disclaimer to the bottom of messages, adding and deleting headers, stripping email attachments, deleting messages, and more. Because individual Content Filter rules are created by the administrator, and because of their diversity, they can be used in many situations and are limited for the most part only be the creativity of the person creating them. With a little bit of thought and experimentation, this feature can be very useful.

MDaemon version 6 has integrated support for MDaemon AntiVirus. Alt-N Technologies, in a joint effort with Kaspersky Labs a world-renowned anti-virus software developer, has developed MDaemon AntiVirus, an anti-virus engine that can be installed and integrated with MDaemon. When MDaemon AntiVirus is installed you will see two additional tabs on the Content Filter dialog. These tabs are used to directly control the plug-in's features and designate what actions MDaemon will take when a virus is detected. To obtain MDaemon AntiVirus, visit `www.altn.com`. See page 177 for more on using MDaemon AntiVirus.

Content Filter Editor



Content filtering rules

☑ Enable rules processing engine

When active, the content filtering system will test all new messages using the rules specified below and perform the requested action if a match is made.

Existing content filter rules

- ☑ Spam Filter
- ☑ Custom Virus Filter
- ☑ X97M.Melissa.A Macro Virus [Move to bad message queue]
- ☑ X97M.Papa.B Macro Virus [Move to bad message queue]
- ☑ ExploreZIP worm [Move to bad message queue]
- ☑ ILOVEYOU worm [Move to bad message queue]
- ☑ X97M.Melissa.A Macro Virus [Remove attachments and append footer]
- ☑ X97M.Papa.B Macro Virus [Remove attachments and append footer]

Click the checkbox to the left of each rule to enable/disable it.
Rule Description: Spam Filter (Enabled)

Apply this rule to messages in the LOCAL & REMOTE queue

If the SUBJECT HEADER contains 'Make $1,000,000 in a day!'
Then Delete this message

All messages processed by MDaemon will at some point reside temporarily in one of the message queues. When Content Filtering is enabled, before any message is allowed to leave the queue it will first be processed through the Content Filter rules. The result of this procedure will determine what is done with the message.

Note

Messages that have a filename beginning with the letter "P" will be ignored by the content filtering process. Every other message will be processed through the content filter system. Once processed, MDaemon will change the first character of the filename to a "P". In this way a message will only be processed through the content filtering system once.

Content Filtering Rules

Enable rules processing engine
Click this checkbox to enable content filtering. All messages processed by MDaemon will be filtered through the content filter rules before being delivered.

Existing Content Filter Rules

This box lists all rules in the order that they will be applied to a message. This makes it possible for you to arrange your rules to achieve a greater level of versatility.

For example: If you have a rule that deletes all messages containing the words, "This is Spam!" and a similar rule that sends those messages to the Postmaster, then putting them in the right order will enable both rules to be applied to the message. This assumes that there isn't a "Stop Processing Rules" rule that applies to the message higher up in the list. If so, then you would use the *Move Up/Move Down* buttons to move the "Stop" rule below the other two. Now any message containing "This is Spam!" would be copied to the Postmaster and then deleted.

Note

Since version 3, MDaemon has had the capability to create rules that will perform multiple tasks and use `and/or` logic. Therefore, considering the example above, you can create a single rule that will accomplish all of those tasks and more.

New rule
Click this button to create a new content filter rule. This will open the Setup New Rule dialog.

Edit rule
Click this button to open the selected rule in the Modify Rule editor.

Copy rule
Click this button to clone the selected content filter rule. An identical rule will be created and added to the list. The new rule will be given a default name called "Copy of [Original Rule Name]". This is useful if you wish to create multiple similar rules. You can create a single rule, clone it several times, and then modify the copies as needed.

Delete rule
Click this button to delete the selected content filter rule. You will be asked to confirm your decision to delete the Rule before MDaemon will do so.

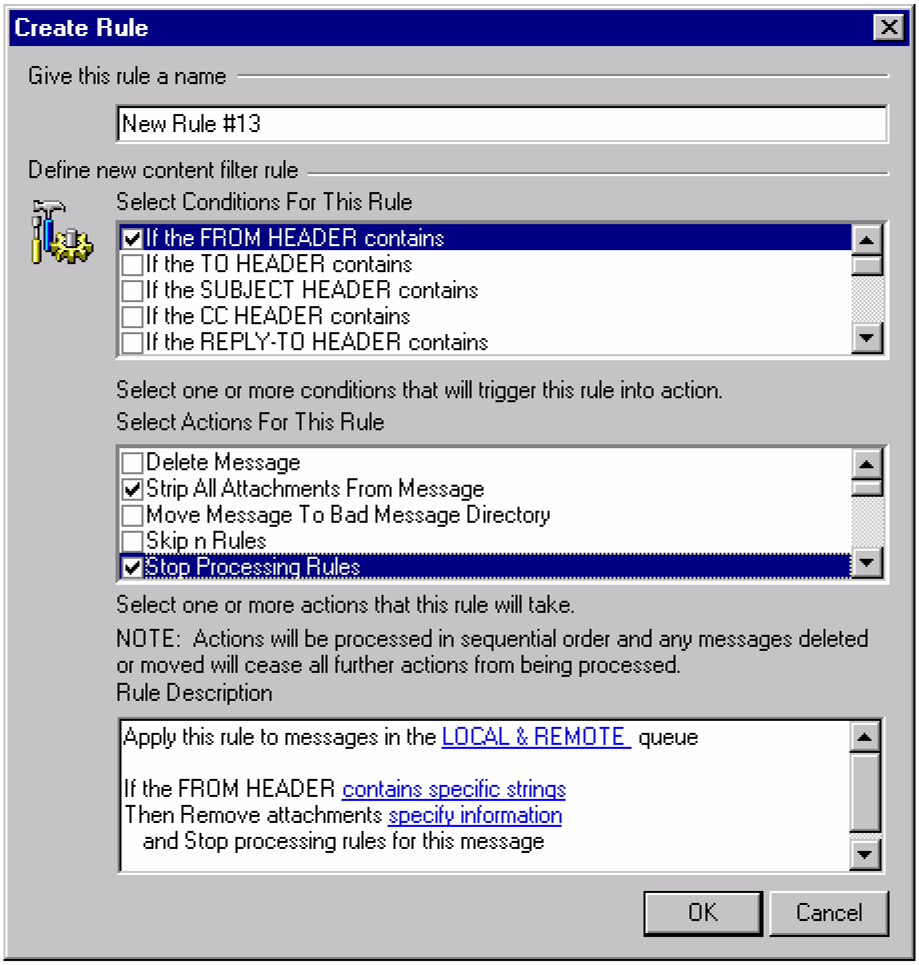
Move up
Click this button to move the selected rule up.

Move down
Click this button to move the selected rule down.

Rule Description [*Rule Name*] (Enabled/Disabled)

This box displays the currently selected rule in its internal script format. Click any of the rule's conditions (listed as a hyperlink) and the appropriate editor will be opened for changing that particular condition.

Creating a New Content Filter Rule



Create Rule

Give this rule a name

New Rule #13

Define new content filter rule

Select Conditions For This Rule

☑ If the FROM HEADER contains
□ If the TO HEADER contains
□ If the SUBJECT HEADER contains
□ If the CC HEADER contains
□ If the REPLY-TO HEADER contains

Select one or more conditions that will trigger this rule into action.

Select Actions For This Rule

□ Delete Message
☑ Strip All Attachments From Message
□ Move Message To Bad Message Directory
□ Skip n Rules
☑ Stop Processing Rules

Select one or more actions that this rule will take.

NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed.

Rule Description

Apply this rule to messages in the LOCAL & REMOTE queue

If the FROM HEADER contains specific strings
Then Remove attachments specify information
and Stop processing rules for this message

This dialog is used for creating Content Filter Rules. It is reached by clicking the *New Rule* button on the Content Filter dialog.

Give This Rule a Name

Type a descriptive name for your new rule here. By default it will be called "New Rule #n".

Define New Content Filter Rule

Select conditions for this rule

This box lists the conditions that may be applied to your new rule. Click the checkbox corresponding to any condition that you want to be applied to the new rule. Each enabled condition will appear in the Rule Description box below. Most Conditions will require additional information that you will specify by clicking on the Condition's hyperlink in the Rule Description box.

> **`If the [HEADER] contains`**—Click any of these options to base your rule on the content of those particular message headers. You must specify the text for which to scan.

If the user defined [# HEADER] contains—Click one or more of these options to base the rule on message headers that you will define. You must specify the new header, and the text for which to scan.

If the MESSAGE BODY contains—This option makes the contents of the message body one of the conditions. This condition requires you to specify a text string for which to search.

If the MESSAGE has Attachment(s)—When this option is selected, the rule will be contingent upon the presence of one or more message attachments. No additional information is required.

If the MESSAGE SIZE is greater than—Click this option if you want the rule to be based upon the size of the message. The size must be specified in *KB*. Default is 10KB.

If the MESSAGE HAS A FILE called—This option will scan for a file attachment with a particular name. The filename must be specified. Wildcards such as `*.exe` and `file*.*` are permitted.

If the MESSAGE IS DIGITALLY SIGNED—The condition applies to messages that have been digitally signed. No further information is required by this condition.

If ALL MESSAGES—Click this option if you want the rule to be applied to all messages. No further information is required; this rule will affect every message except those to which a "Stop Processing Rules" or "Delete Message" action has been applied in a previous rule.

Select actions for this rule

MDaemon can perform these actions if a message matches the rule's conditions. A few Actions will require additional information that you will specify by clicking on the Action's hyperlink in the Rule Description box.

Delete Message—Selecting this action will cause the message to be deleted.

Strip All Attachments From Message—This action causes all attachments to be stripped from the message.

Move Message To Bad Message Directory—Click this action to cause a message to be moved to the bad message directory.

Skip n Rules—Selecting this action will cause a specified number of rules to be skipped. This is useful in situations where you may want a rule to be applied in certain circumstances but not in others.

For example: you may wish to delete messages that contain the word "Spam", but not those that contain "Good Spam". To accomplish this you could create a rule that deletes messages containing "Spam" and then place above it another rule that states "if the message contains "Good Spam" then Skip 1 Rule".

Stop Processing Rules—This action will skip all remaining rules.

Copy Message To Specified User(s)—Causes a copy of the message to be sent to one or more recipients. You must specify which recipients are to receive the message.

Append Standard Disclaimer—This action makes it possible for you to create a small amount of text that will be appended as a footer to the message. Alternatively, it can add the contents of a text file.

For example: you could use this rule to include a statement that says "This email originated from my company, please direct any complaints or questions to me@mycompany.com".

Add Extra Header Item To Message—This action will add an additional header to the message. You must specify the name of the new header and its value.

Delete A Header Item From Message—This action will remove a header from a message. You must specify the header that you wish to delete.

Send Note To... —This action will send an email to a particular address. You will be able to specify the recipient, sender, subject, and a small amount of text. You can also configure this action to attach the original message to the note.

For example: you might wish to create a rule that will move all messages containing "This is Spam!" to the bad message directory and create another rule that will send a note to someone letting them know that this has been done.

Remove Digital Signature—Click this action to cause a digital signature to be removed from the message.

Run Process...—This action can be used to run a particular program when a message meets the rule's conditions. You must specify the path to the program that you wish to run. You can use the $MESSAGEFILENAME$ macro to pass the name of the message to the process, and you can specify whether or not MDaemon should suspend its operations temporarily or indefinitely while it waits for the process to terminate. Further, you can force the process to terminate and/or run it in a hidden window.

Send Message Through SMS Gateway Server...—Click this option to send the message through an SMS Gateway Server. You must supply the Host or IP Address and the SMS phone number.

Copy Message to Folder...—Use this option to place a copy of the message into a specific folder.

Add Line To Text File—This option will cause a line of text to be added to a specific text file. When choosing this action you will have to specify the path to the file and the text that you want to be appended to it. You may use certain MDaemon macros in your text to cause the content filter to dynamically include information about the message such as the sender, recipient, message ID, and so on. Click the Macros button on the "Add line to text file" dialog to display a list of permitted macros.

Move Message to Public Folders...—Use this action to cause the message to be moved to one or more Public Folders (page 102).

Search and Replace Words in a Header—Use this option to scan a specified header for certain words and then delete or replace them. When creating this rule, click the "specify information" link in the Rule Description to open the "Header – Search and Replace" dialog on which you will designate the header and words to replace or delete.

`Jump to Rule`...—Use this action to jump immediately to a rule further down in the list, skipping over all rules between the two.

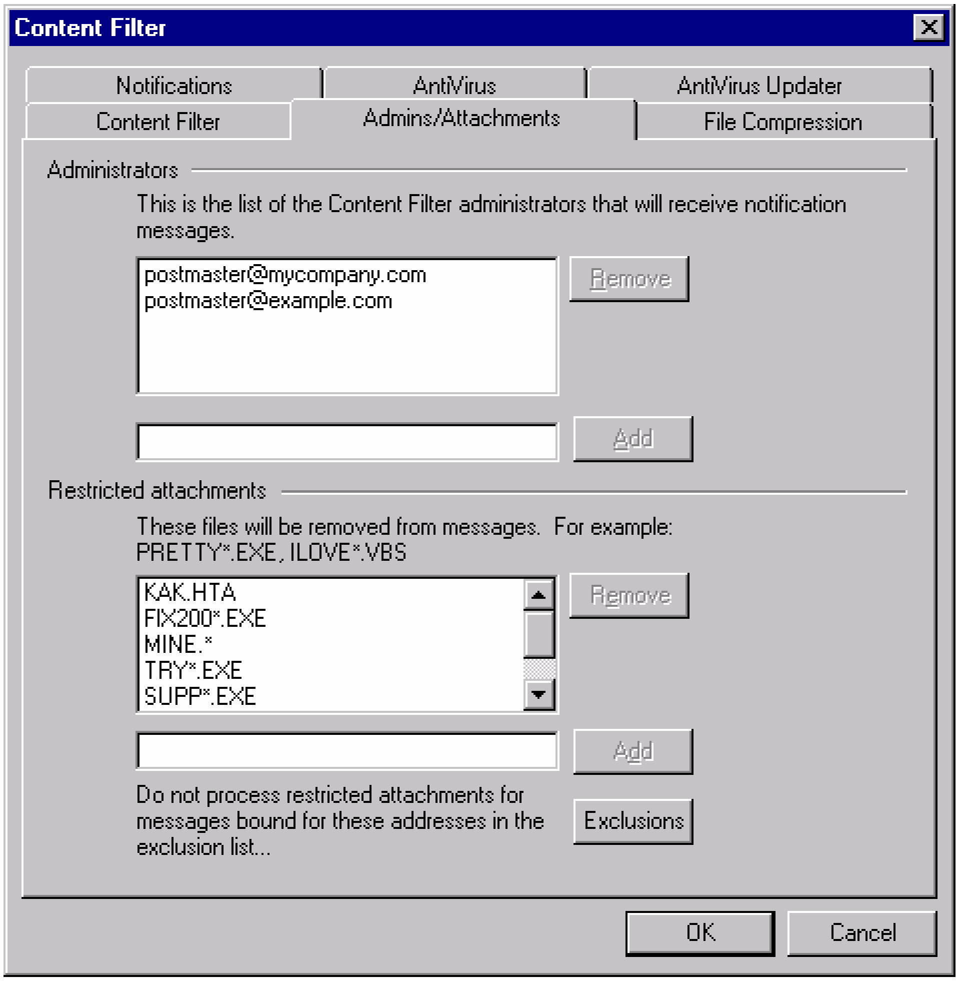
Rule description

This box displays the new rule's internal script format. Click any of the rule's conditions or actions (listed as hyperlinks) and the appropriate editor will be opened for specifying any needed information.

Modifying an Existing Content Filter Rule

To modify an existing content filter rule, select the rule and then click the *Edit Rule* button on the Content Filter dialog. The rule will be opened for editing in the Modify Rule editor. The controls on this editor are identical to the Create Rule Dialog.

Admins/Attachments



This is the list of the Content Filter administrators that will receive notification messages.

postmaster@mycompany.com
postmaster@example.com

These files will be removed from messages. For example: PRETTY*.EXE, ILOVE*.VBS

KAK.HTA
FIX200*.EXE
MINE.*
TRY*.EXE
SUPP*.EXE

Do not process restricted attachments for messages bound for these addresses in the exclusion list...

Use this tab to specify attachments that you wish to classify as restricted and automatically remove from messages. There is also a section that corresponds to the Notifications tab used for designating email addresses as administrators.

Administrators

Addresses listed in this area are considered administrators and correspond to the Administrator controls located on the Notifications tab. These addresses will receive notification messages when one of the Administrator options is selected on that tab. To add an address to this section, type it into the space provided and then click Add. To remove an address, select it from the list and then click Remove.

Restricted Attachments

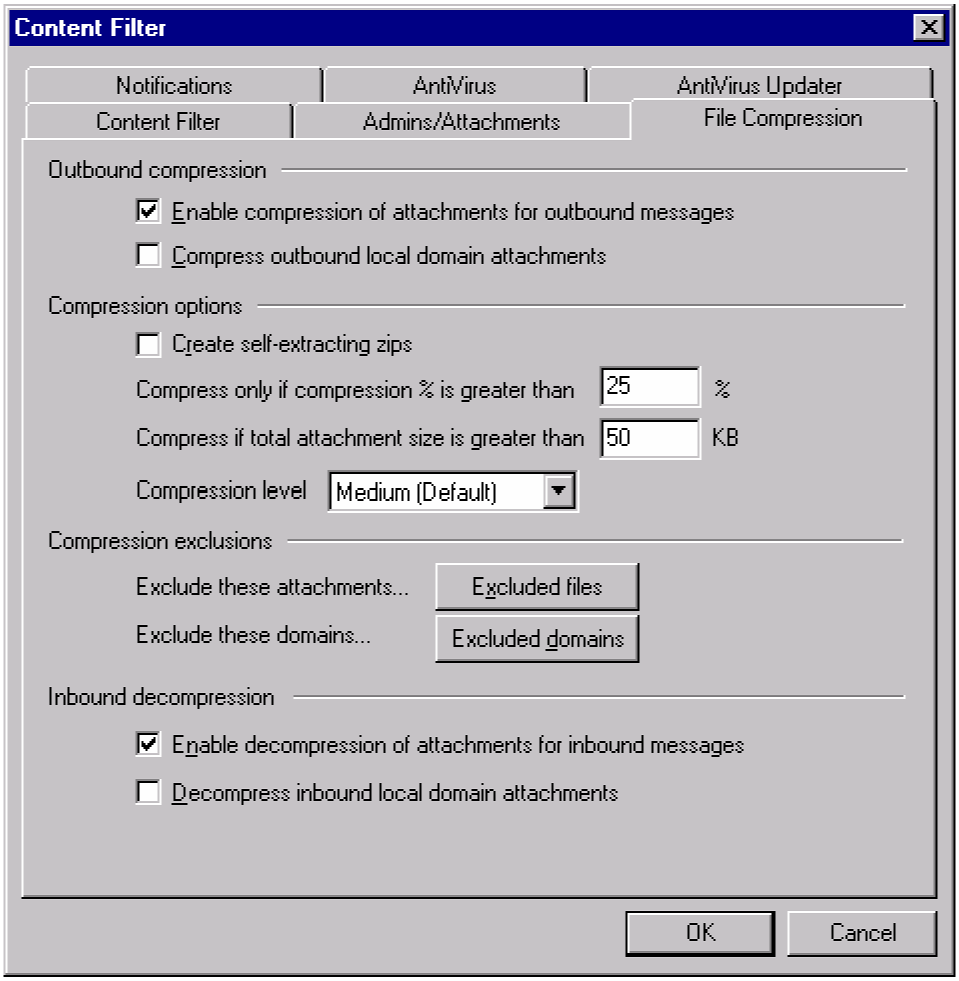
Filenames specified in this list will be stripped from messages automatically when MDaemon encounters them. After the attachment is stripped, MDaemon will continue normally and delivery the message without it. You can use the controls on the Notifications tab to cause a notification message to be sent to various addresses when one of these restricted attachments is encountered.

Wildcards are permitted in list entries. An entry of "`*.exe`", for example, would cause all attachments ending with the `EXE` file extension to be removed. To add an entry to the list, type the filename in the space provided and the click Add.

Exclusions

Click Exclusions to specify addresses that you wish to exclude from attachment restriction monitoring. When a message is directed to one of these addresses MDaemon will allow the message to pass even if it contains a restricted attachment.

File Compression



Outbound compression

☑ Enable compression of attachments for outbound messages

□ Compress outbound local domain attachments

Compression options

□ Create self-extracting zips

Compress only if compression % is greater than 25 %

Compress if total attachment size is greater than 50 KB

Compression level Medium (Default)

Compression exclusions

Exclude these attachments...

Exclude these domains...

Inbound decompression

☑ Enable decompression of attachments for inbound messages

□ Decompress inbound local domain attachments

With the controls on this tab you can cause message attachments to be automatically compressed or decompressed before the message is delivered. The level of compression can be controlled as well as several other parameters and exclusions. This feature could significantly reduce the amount of bandwidth and throughput required to deliver your outbound messages.

Outbound Compression

Enable compression of attachments for outbound messages

Click this checkbox if you want to enable automatic message attachment compression for outbound remote mail messages. Enabling this control will not cause all message attachments to be compressed; it simply turns the feature on. Whether an outbound message's files are compressed or not is determined by the remaining settings on this tab.

Compress outbound local domain attachments

Enabling this control will cause the file compression settings to be applied to all outbound mail – even those messages whose destination is another local address.

Compression Options

Create self-extracting zips

Click this checkbox if you want the compression files that MDaemon creates to be self-extracting zip files with an EXE file extension. This is useful if you are concerned that the message recipients may not have access to a decompression utility. Self-extracting zip files can be decompressed simply by double-clicking on them.

Compress only if compression % is greater than XX%

MDaemon will not compress a message's attachments before sending it unless they can be compressed by a percentage greater than the value specified in this control. For example, if you designate a value of 20 and a given attachment can't be compressed by at least 21% then MDaemon will not compress it before sending the message.

Note

MDaemon must first compress a file to determine by what percentage it can be compressed. Thus, this feature does not prevent files from being compressed – it simply prevents file attachments from being sent in a compressed format when they cannot be compressed beyond the designated value. In other words, if after compressing the file MDaemon finds that it couldn't be compressed by more than this value, the compression will be disregarded and the message will be delivered with its attachments unchanged.

Compress if total attachment size is greater than XX KB

When automatic attachment compression is enabled, MDaemon will only attempt to compress a message's attachments when their total size exceeds the value specified here. Messages with total attachment sizes below this threshold will be delivered normally with the attachments unchanged.

Compression level

Use the drop-down list box to choose the degree of compression that you want MDaemon to apply to automatically compressed attachments. You can choose three levels of compression: minimum (fastest compression process with least compression), medium (default value), or maximum (slowest compression process but highest degree of compression).

Compression exclusions

Exclude these attachments…

Click this button to specify files that you want to exclude from the automatic compression features. When a message attachment matches one of these filenames it will not be compressed, regardless of the compression settings. Wildcards are permitted in these entries. Therefore, you could specify "*.exe", for example, and all files ending with ".exe" would remain uncompressed.

Exclude these domains…

Click this button to specify recipient domains whose messages you wish to exclude from automatic compression. Messages bound for these domains will not have their file attachments compressed, regardless of your compression settings.

Inbound Decompression

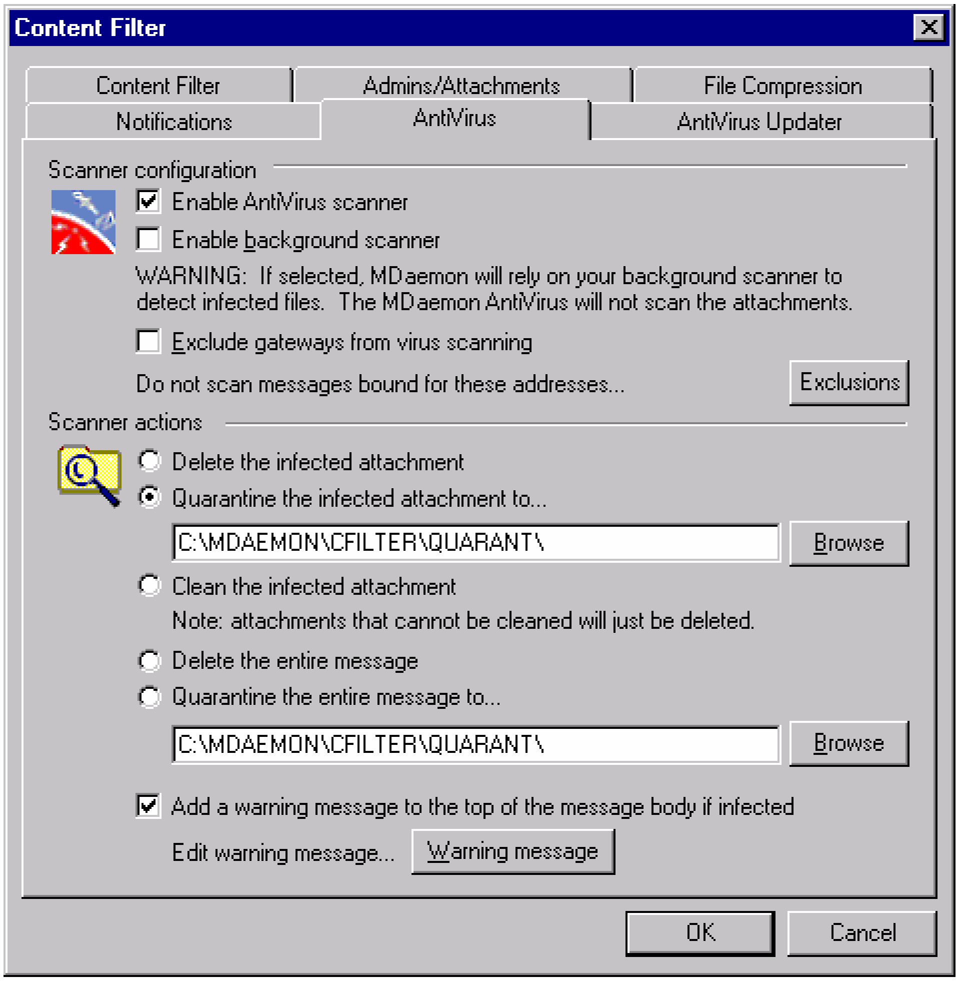
Enable decompression of attachments for inbound messages

Click this checkbox if you want to enable automatic decompression of inbound remote mail message attachments. When a message arrives with a zipped attachment, MDaemon will decompress it before delivering it to the local user's mailbox.

Decompress inbound local domain attachments

Enable this control if you want automatic decompression to apply to local mail as well.

AntiVirus



Scanner configuration

☑ Enable AntiVirus scanner

☐ Enable background scanner

WARNING: If selected, MDaemon will rely on your background scanner to detect infected files. The MDaemon AntiVirus will not scan the attachments.

☐ Exclude gateways from virus scanning

Do not scan messages bound for these addresses...

Scanner actions

○ Delete the infected attachment

● Quarantine the infected attachment to...

C:\MDAEMON\CFILTER\QUARANT\

○ Clean the infected attachment

Note: attachments that cannot be cleaned will just be deleted.

○ Delete the entire message

○ Quarantine the entire message to...

C:\MDAEMON\CFILTER\QUARANT\

☑ Add a warning message to the top of the message body if infected

Edit warning message...

This tab (and the AntiVirus Updater tab) will only be visible when you have installed MDaemon AntiVirus. To obtain MDaemon AntiVirus, visit www.altn.com.

Scanner Configuration

Enable virus scanner

Click this checkbox to enable AntiVirus scanning of messages. When MDaemon receives a message with attachments, it will activate MDaemon AntiVirus and scan them for viruses before delivering the message to its final destination.

Enable background scanner

If you have a background virus scanner installed on your system, enable this control if you want to allow background scanning of messages instead of scanning them with MDaemon AntiVirus.

Warning!

Because this feature prevents MDaemon AntiVirus from scanning your messages directly, using it may have unpredictable results. For this reason, we recommend that you configure your background scanner to exclude the MDaemon folders from monitoring, disable this control, and allow MDaemon AntiVirus to handle the scanning of your message attachments directly.

<u>Exclude gateways from virus scanning</u>

Click this checkbox if you want messages bound for one of MDaemon's domain gateways to be excluded from virus scanning. This may be desirable for those who wish to leave the scanning of those messages to the domain's own mail server. For more information on domain gateways, see Domain Gateways – page 288.

<u>Do not scan messages bound for these addresses…Exclusions</u>

Click the *Exclusions* button to specify recipient addresses to exclude from virus scanning. Messages bound for these addresses will not be scanned for viruses by MDaemon AntiVirus. Wildcards are allowed in these addresses. You could therefore use this feature to exclude entire domains or specific mailboxes across all domains. For example, "*@example.com or "VirusArchive@*".

Scanner Actions

Click one of the option buttons in this section to designate the action that MDaemon will take when MDaemon AntiVirus detects a virus.

<u>Delete the infected attachment</u>

This option will delete the infected attachment. The message will still be delivered to the recipient but without the infected attachment. You can use the "*Add a warning…*" control on the bottom of this dialog to add text to the message informing the user that an infected attachment was deleted.

<u>Quarantine the infected attachment to…</u>

Choose this option and specify a location in the space provided if you want infected attachments to be quarantined to that location rather than deleted or cleaned. Like the "*Delete the infected attachment*" option, the message will still be delivered to the recipient but without the infected attachment.

<u>Clean the infected attachment</u>

When this option is chosen, MDaemon AntiVirus will attempt to clean, or disable, the infected attachment. If the attachment cannot be cleaned, it will be deleted.

<u>Delete the entire message</u>

This option will delete the entire message rather than just the attachment when a virus is found. Because this deletes the whole message, the "*Add a warning…*" option doesn't apply. However, you can still send a notification message to the recipient by using the controls on the Notifications tab.

<u>Quarantine the entire message to…</u>

This option is like the "*Delete the entire message*" option above, but the message will be quarantined in the specified location rather than deleted.

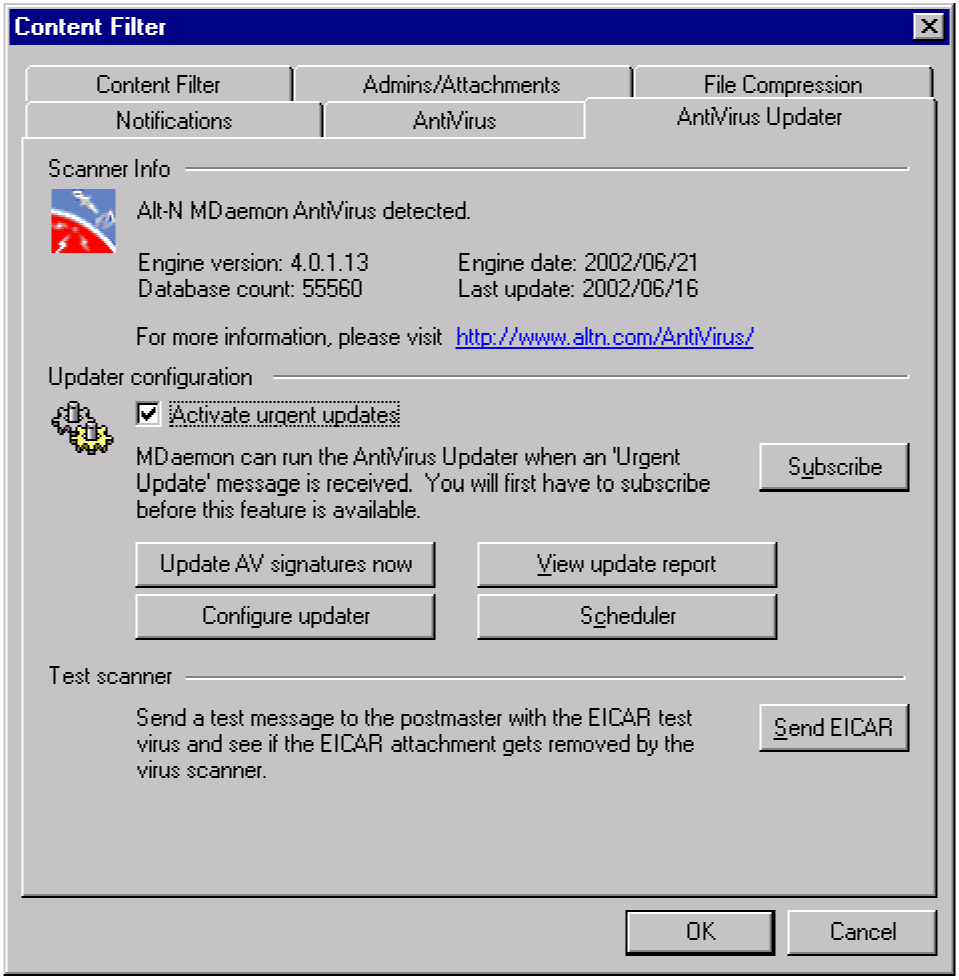
<u>Add a warning message to the top of the message body if infected</u>

When one of the "*…attachment*" options is chosen above, click this option if you want to add some warning text to the top of the previously infected message before it is delivered to the recipient. Thus you can inform the recipient that the attachment was stripped and why.

Edit warning message…

Click this button to display the warning text that will be added to messages when the "*Add a warning message…*" feature is used. After making any desired changes to the text, click "OK" to close the dialog and save the changes.

AntiVirus Updater



Alt-N MDaemon AntiVirus detected.

Engine version: 4.0.1.13 Engine date: 2002/06/21
Database count: 55560 Last update: 2002/06/16

For more information, please visit http://www.altn.com/AntiVirus/

☑ Activate urgent updates

MDaemon can run the AntiVirus Updater when an 'Urgent Update' message is received. You will first have to subscribe before this feature is available.

Send a test message to the postmaster with the EICAR test virus and see if the EICAR attachment gets removed by the virus scanner.

Use the controls on this tab to manually or automatically update MDaemon AntiVirus' virus definitions. There is a scheduler for automatic updating, a report viewer so that you can review when and which updates have been downloaded, and a test feature used for confirming that you your virus scanning is working properly.

Scanner info

This section tells you whether MDaemon AntiVirus is installed and, if so, what version you are running. It also lists the date of your last virus definition update.

Updater Configuration

<u>Activate urgent updates</u>

Click this checkbox to activate the urgent updates feature. With this feature enabled, AntiVirus will immediately connect to the update location and download the high-priority update whenever MDaemon receives an "Urgent Update" message. To receive these messages you must first subscribe to the "Urgent Updates" mailing list. See the *Subscribe* control below.

Subscribe

This button to opens your default browser to Alt-N Technologies' Urgent Updates subscription page. On that page enter your domain name to subscribe your domain to the Urgent Updates mailing list. Whenever there is an urgent update to MDaemon AntiVirus's virus definitions, an email will be dispatched to the domain. When MDaemon receives the message MDaemon AntiVirus will be updated immediately.

Update AV signatures now

Click this button to update the virus definitions manually. The updater will connect immediately after the button is pressed.

Configure updater

Click this button to open the updater. The Updater contains three tabs: Update URLs, Connection, and Proxy.

The Update URLs tab contains a list of sites to which MDaemon AntiVirus will connect to check for virus signature updates. You can add and remove web sites to and from the list, and move the URLs up and down in the list by using the provided arrow buttons; the web sites are checked for updates from top to bottom. Clicking the control, "*Use random starting point in the URL list*" will cause the sites to be checked in random order rather than in the order that they are listed.

The Connection tab is used to designate the Internet Connection Profile that you wish MDaemon AntiVirus to use when connecting to the update sites. The "*Use Internet Settings from Control Panel*" option uses your default Internet settings. The "*Setup Internet settings manually*" option and subsequent controls can be used to manually choose a Connection Profile and designate its user name and password settings.

The Proxy tab contains options for configuring any HTTP or FTP proxy settings that your current network configuration may require in order to connect to the update sites.

View update report

The MDaemon AntiVirus Log Viewer is opened by clicking the *View update report* button. The viewer lists the times, actions taken, and other information about each update.

Scheduler

Click this button to open MDaemon's Event Scheduler to the AntiVirus Updates tab. The controls on this tab are similar to those on the Send & Receive Mail tab and can be used to schedule checks for virus signature updates at specific times on specific days or by a Simple Scheduling method that causes MDaemon AntiVirus to check for updates once every so many minutes. There is also an *Activate urgent updates* option on this tab that can be used to activate or deactivate Automatic Urgent Updates. This option is the same as the control of the same name described above.

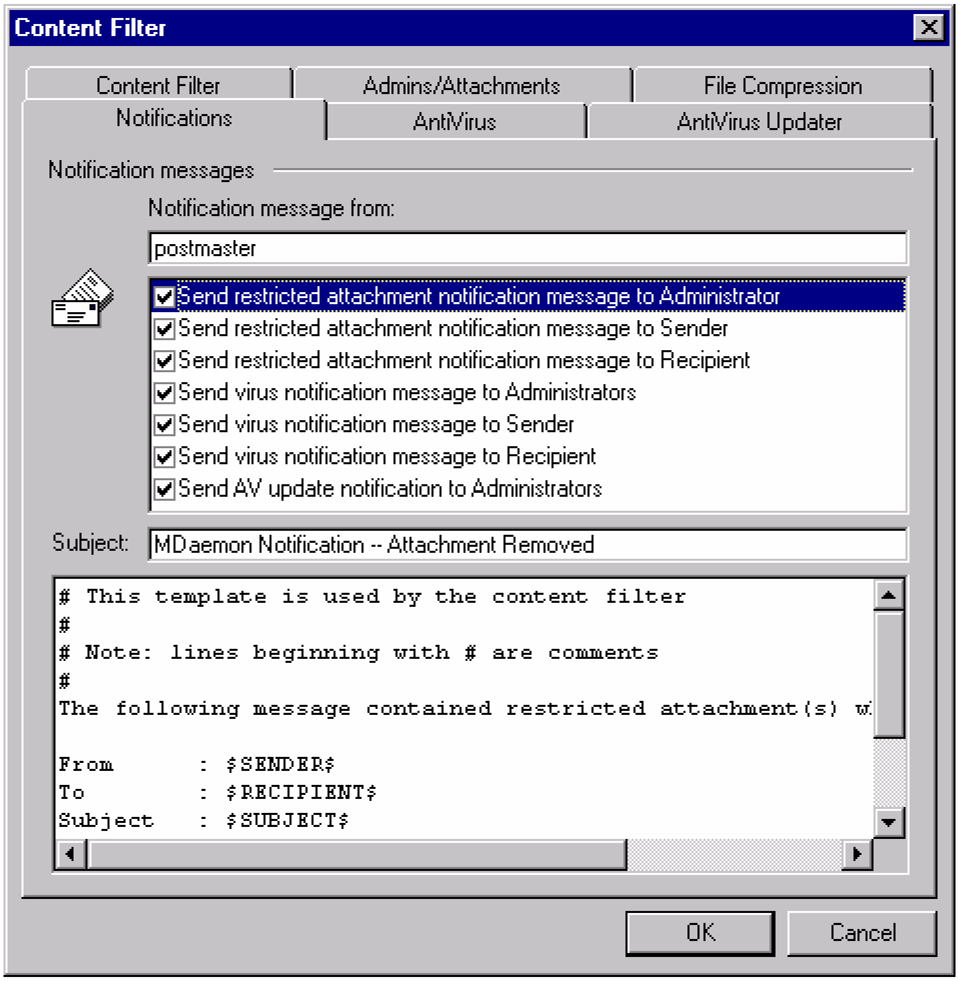
Test Scanner

Send EICAR

Click this button to send a test message to the postmaster, with the EICAR virus file attached. This attachment is harmless – it is merely used to test MDaemon AntiVirus. By watching the Content Filter's log window on MDaemon's main interface you can see what MDaemon does with this message when it is received. For example, depending upon your settings, you might see a log excerpt that looks something like this:

```
Mon 2002-02-25 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 2002-02-25 18:14:49: > eicar.com
(C:\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 2002-02-25 18:14:49: > Message from: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message to: postmaster@mycompany.com
Mon 2002-02-25 18:14:49: > Message subject: EICAR Test Message
Mon 2002-02-25 18:14:49: > Message ID:
<MDAEMON10001200202251814.AA1447619@mycompany.com>
Mon 2002-02-25 18:14:49: Performing viral scan...
Mon 2002-02-25 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 2002-02-25 18:14:50: > eicar.com was removed from message
Mon 2002-02-25 18:14:50: > eicar.com quarantined to
C:\MDAEMON\CFILTER\QUARANT\
Mon 2002-02-25 18:14:50: > Total attachments scanned    : 1 (including
multipart/alternatives)
Mon 2002-02-25 18:14:50: > Total attachments infected   : 1
Mon 2002-02-25 18:14:50: > Total attachments disinfected: 0
Mon 2002-02-25 18:14:50: > Total attachments removed    : 1
Mon 2002-02-25 18:14:50: > Total errors while scanning  : 0
Mon 2002-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (sender)
Mon 2002-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (recipient)
Mon 2002-02-25 18:14:50: > Virus notification sent to
postmaster@mycompany.com (admin)
Mon 2002-02-25 18:14:50: > Virus notification sent to postmaster@example.com
(admin)
Mon 2002-02-25 18:14:50: Processing complete (matched 0 of 12 active rules)
```

Notifications



Notification messages

Notification message from: postmaster

- ☑ Send restricted attachment notification message to Administrator
- ☑ Send restricted attachment notification message to Sender
- ☑ Send restricted attachment notification message to Recipient
- ☑ Send virus notification message to Administrators
- ☑ Send virus notification message to Sender
- ☑ Send virus notification message to Recipient
- ☑ Send AV update notification to Administrators

Subject: MDaemon Notification -- Attachment Removed

```
# This template is used by the content filter
#
# Note: lines beginning with # are comments
#
The following message contained restricted attachment(s) w

From      : $SENDER$
To        : $RECIPIENT$
Subject   : $SUBJECT$
```

Use this tab to designate those whom should receive notification messages when a virus or restricted attachment is detected.

Notification Messages

Notification message from:
Use this control for specifying the address from which you want the notification message to come.

Send virus notification message to…
When a message arrives with a file attachment containing a virus, a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have designated on the Admins/Attachments tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

Send restricted attachment notification message to…
When a message arrives with a file attachment matching a restricted attachment entry (listed on the Admins/Attachments tab) a warning message will be sent to the individuals designated in this section. A customized warning message can be sent to the sender, recipient, and the administrators that you have

designated on the Admins/Attachments tab. To customize the message for any of the three entries, select one of them from the list and then edit the message that appears on the bottom half of this tab. Each entry has its own message, though by default this isn't obvious since all three are identical.

Subject
This text will be displayed in the "Subject:" header of the notification message that is sent.

Message
This is the message that will be sent to the entry selected in the list above when the checkbox corresponding to that entry is enabled. You can directly edit this message from the box in which it is displayed.

Note

The actual files containing this text are located in the `MDaemon\app\` directory. They are:

`cfattrem[adm].dat`	Restricted attachment message – Admins
`cfattrem[rec].dat`	Restricted attachment message – Recipient
`cfattrem[snd].dat`	Restricted attachment message – Sender
`cfvirfnd[adm].dat`	Virus found message – Admins
`cfvirfnd[rec].dat`	Virus found message – Recipient
`cfvirfnd[snd].dat`	Virus found message – Sender

Should you desire to restore one of these messages to its original appearance, simply delete the relevant file and MDaemon will recreate it in its default state.

Message Macros

For your convenience, certain macros may be used in the notification messages and other messages that the Content Filters generate. You may use any of the following macros, many of which are listed on page 264:

`$ACTUALTO$`
Some messages may contain an "ActualTo" field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation. This macro is replaced with that value.

`$CURRENTTIME$`
This macro is replaced with the current time when the message is being processed.

`$ACTUALFROM$`
Some messages may contain an "ActualFrom" field which generally represents the origination mailbox and host prior to any reformatting or alias translation. This macro is replaced with that value.

`$FILTERRULENAME$`
This macro is replaced by the name of the rule whose criteria the message matched.

`$HEADER:XX$`
This macro will cause the value of the header specified in place of the "xx" to be expanded in the reformatted message. For example: If the original message has "TO: joe@mdaemon.com" then the

	$HEADER:TO$ macro will expand to “joe@mdaemon.com”. If the original message has “Subject: This is the subject” then the $HEADER:SUBJECT$ macro would be replaced with the text “This is the subject”
`$HEADER:MESSAGE-ID$`	As with `$HEADER:XX$` above, this macro will expand to the value of the `Message-ID` header.
`$LIST_ATTACHMENTS_REMOVED$`	When one or more attachments are removed from the message, this macro will list them.
`$LIST_VIRUSES_FOUND$`	When one or more viruses is found in a message, this macro will list them.
`$MESSAGEFILENAME$`	This macro expands to the file name of the current message being processed.
`$MESSAGEID$`	As `$HEADER:MESSAGE-ID$` above, except this macro strips “<>” from the value of the message ID.
`$PRIMARYDOMAIN$`	Expands to MDaemon’s primary domain name, which is designated on the Primary Domain Configuration dialog (click Setup | Primary Domain).
`$PRIMARYIP$`	This macro expands to the IP address of your primary domain (specified on the Primary Domain Configuration dialog)
`$RECIPIENT$`	This macro resolves to the full address of the message recipient.
`$RECIPIENTDOMAIN$`	This macro will insert the domain name of the message recipient.
`$RECIPIENTMAILBOX$`	Lists the recipient’s mailbox (the value to the left of “@” in the email address).
`$REPLYTO$`	This macro expands to the value of the message’s “Reply-to” header.
`$SENDER$`	Expands to the full address from which the message was sent.
`$SENDERDOMAIN$`	This macro will insert the domain name of the message’s sender (the value to the right of “@” in the email address).
`$SENDERMAILBOX$`	Lists the sender’s mailbox (the value to the left of “@” in the email address).
`$SUBJECT$`	Displays the text contained in the message’s subject.

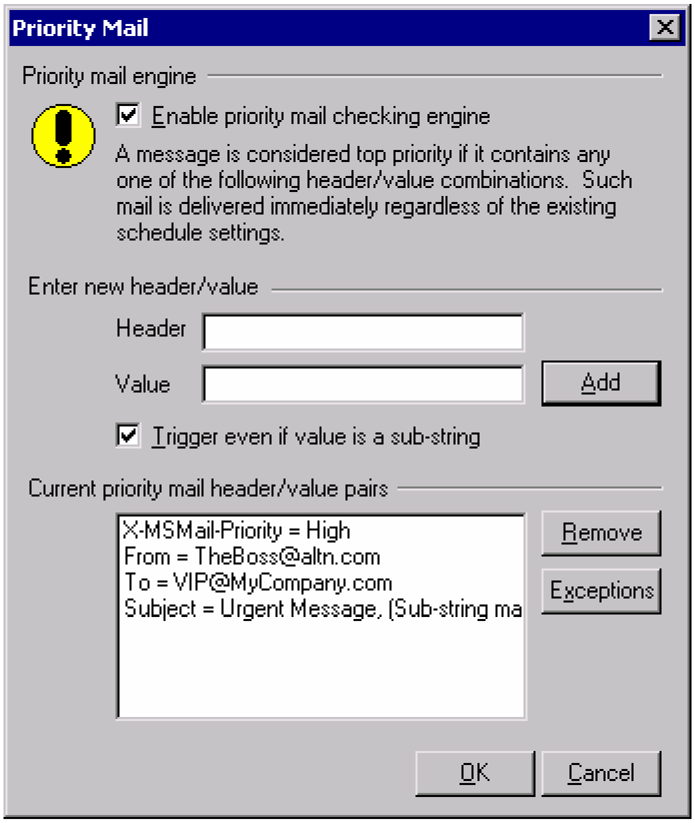
Chapter 15

Priority Mail

Configuring and using the Priority Mail feature.

The **Setup | Priority Mail…** menu selection opens the Priority Mail dialog, which is used to define what constitutes Priority Mail on your system. Priority mail is delivered immediately by MDaemon regardless of scheduled mail processing intervals. When a new message arrives, MDaemon inspects its headers for a set of header/value combinations that you have specified on this dialog. If it finds them, it considers the message a high priority item and attempts to deliver it immediately.

Priority Mail



☑ Enable priority mail checking engine

A message is considered top priority if it contains any one of the following header/value combinations. Such mail is delivered immediately regardless of the existing schedule settings.

☑ Trigger even if value is a sub-string

```
X-MSMail-Priority = High
From = TheBoss@altn.com
To = VIP@MyCompany.com
Subject = Urgent Message, (Sub-string ma
```

Priority Mail Engine

Enable priority mail checking engine

Click this switch to enable the Priority Mail feature. MDaemon will inspect incoming messages for priority status.

Enter New Header/Value

Header
Enter the message header in this field. Do not include the ending colon character.

Value
Enter the value that must be found in the specified header in order for the message to be considered high priority.

Trigger even if value is a sub-string
When entering a new Priority Mail setting you may select this feature to enable priority matching of a portion (or sub-string) of a header value. For example, you could create a Priority Mail Setting for the "`To`" header with the value "`Boss`". Then, any email containing "`Boss@anything`" in that header would be considered Priority Mail. If an entry is created without this feature enabled then the value of the header must match the entry exactly; matching only a portion will not be sufficient.

Add
After entering the Header/Value information in the specified text boxes, and after specifying whether this entry will apply to sub-strings, click the *Add* button to create the new Priority Mail entry.

Current Priority Mail Header/Value Pairs

This window lists all the currently defined priority mail header/value combinations. Double click on an item in this list to remove it.

Remove
Click this button to remove a selected entry from the *Current Priority Mail Settings* window.

Exceptions
This allows you to define field/value combinations that will cause a message to be considered an exception to the priority mail settings. This gives you more flexible control over this feature.

Chapter

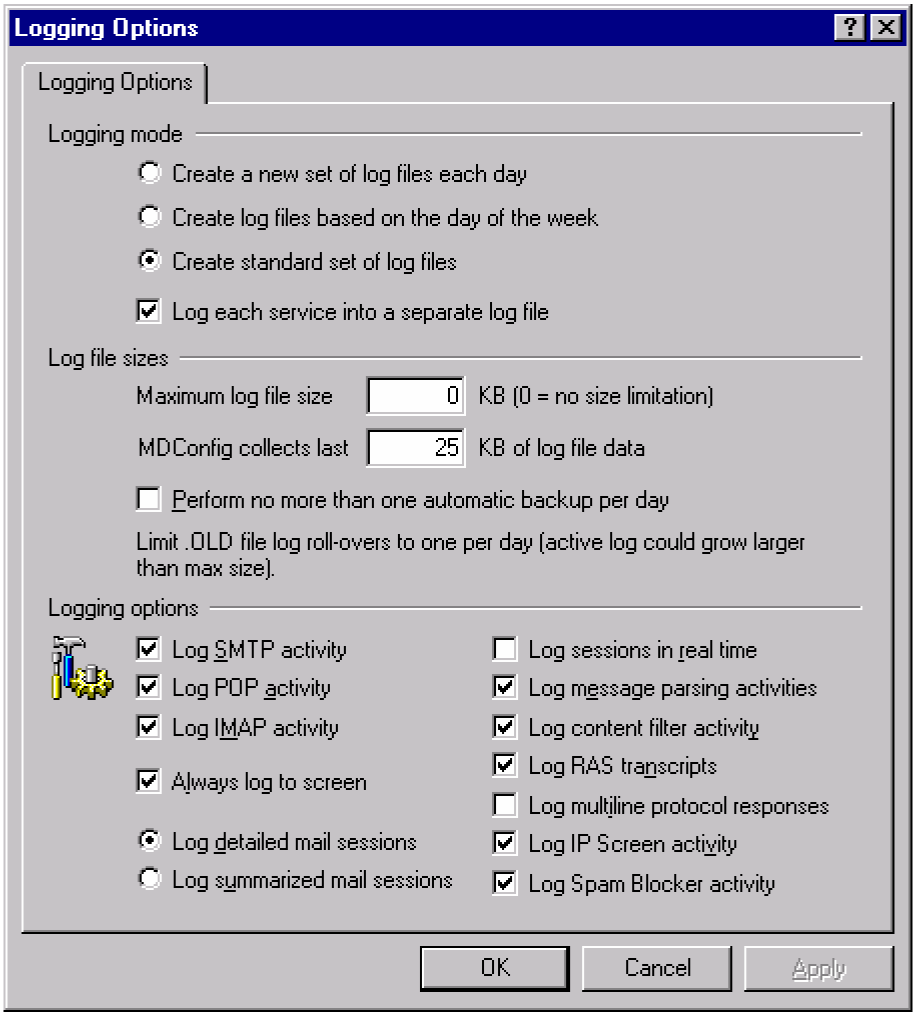
16

Logging

Configuring MDaemon's Logging options.

Click the **Setup | Logging options…** menu selection to configure your Log File settings. The log file is a useful tool for diagnosing problems and seeing what the server has been doing while unattended.

Logging



Logging Options

Logging Options

Logging mode

○ Create a new set of log files each day

○ Create log files based on the day of the week

● Create standard set of log files

☑ Log each service into a separate log file

Log file sizes

Maximum log file size 0 KB (0 = no size limitation)

MDConfig collects last 25 KB of log file data

□ Perform no more than one automatic backup per day

Limit .OLD file log roll-overs to one per day (active log could grow larger than max size).

Logging options

☑ Log SMTP activity

☑ Log POP activity

☑ Log IMAP activity

☑ Always log to screen

● Log detailed mail sessions

○ Log summarized mail sessions

□ Log sessions in real time

☑ Log message parsing activities

☑ Log content filter activity

☑ Log RAS transcripts

□ Log multiline protocol responses

☑ Log IP Screen activity

☑ Log Spam Blocker activity

Note

There are several controls on the Miscellaneous Options dialog governing the amount of log data that may be displayed in the router window of MDaemon's main interface. For more information, see Miscellaneous Options – GUI on page 194.

Logging Mode

Create a new set of log files each day

If this option is selected then separate log files will be generated each day. The name of the files will be correspond to the date they were created.

Create log files based on the day of the week

If this option is selected, separate log files will be generated for each day of the week. The name of the log files will correspond to the day of the week on which they were created.

Create standard set of log files

Click this option to maintain a standard single set of log files.

Log each service into a separate log file

Click this checkbox to cause MDaemon to maintain separate logs by service rather than in a single file. For example, with this switch set MDaemon will log SMTP activity in the `MDaemon-SMTP.log` file and IMAP activity in the `MDaemon-IMAP.log` file. This option must be selected when you are running a "ghost" or Terminal Services instance of MDaemon in order for the tabs on the interface to display the logged information.

Log File Sizes

Max log file size [xx] KB

This is the maximum size in kilobytes that a log file may reach. Once this size is reached, the log file is `copied` to `LOGFILENAME.OLD` and a new log is started.

MDConfig collects last [xx] KB of log file data

When using MDConfig to configure MDaemon remotely, this amount of data will be copied from the bottom of MDaemon's current log files and displayed in MDConfig's interface.

Perform no more than one automatic backup per day

When limiting the log file size, click this checkbox if you want no more than one log file to be backed up per day. Each day, the first time that the maximum log file size is reached it will be renamed to "`*.OLD`" and saved normally. The subsequent log file will continue to grow regardless of the maximum size specified. It will not be rolled over until the next day—even if the maximum size setting is surpassed.

Logging Options

Log SMTP activity

Enable this option if you want to log all of MDaemon's send/receive SMTP activity.

Log POP activity

Click this checkbox to log all POP mail activity. This will log your users' POP mail collection sessions from MDaemon, and will log MDaemon's DomainPOP and MultiPOP activity.

Log IMAP activity

Enabling this option causes all of your users' IMAP sessions to be included in MDaemon's log files.

Always log to screen

Click this option if you want the logged data to be copied to the MDaemon GUI even when it is minimized or running in the tray.

When this control is cleared, log data isn't copied to the router window when MDaemon is running in the system tray. Consequently, the most recent activity won't be listed on any of the router window's tabs when MDaemon is first opened. The router will begin displaying newly logged information from that point forward.

Log detailed mail sessions

A complete transcript of each mail transaction session will be copied to the log file when this option is active.

Log summarized mail sessions

The option causes a summarized transcript of each mail transaction session to be copied to the log file.

Log sessions in real time

Ordinarily, session information is logged after the session is completed in order to conserve resources. Click this option if you want session information to be logged as in occurs.

Log message parsing activities

MDaemon periodically performs a great deal of message parsing activity when determining to whom a message should be delivered. Enable this switch if you want this information to be included in the log file.

Log content filter activity

Click this checkbox if you want to include Content Filter and MDaemon AntiVirus activity in the log file.

Include RAS transcripts

Click this switch if you want MDaemon to copy RAS dialup/dialdown activities into the log file. This information is useful for diagnosing dialup problems.

Log multi-line protocol responses

Sometimes the responses to protocol requests require more than one line of information. Click this checkbox if you want to log these additional lines.

Caution!

Enabling this switch could potentially increase the amount of logged information a great deal. Because the number of lines in a response can't be determined in advance, and because some responses have great potential for "filling up" your log file with possibly unnecessary information (POP TOP, for example, which lists the actual contents of the message), we do not recommend using this feature if log file size or verbosity is of concern to you.

Log IP Screen activity

Click this checkbox if you want the IP Screening activities to be included in MDaemon's log file.

Log Spam Blocker activity

This option causes MDaemon to log Spam Blocker activity. Using this option will allow you to have an easy reference to the sites that were logged as blacklisted.

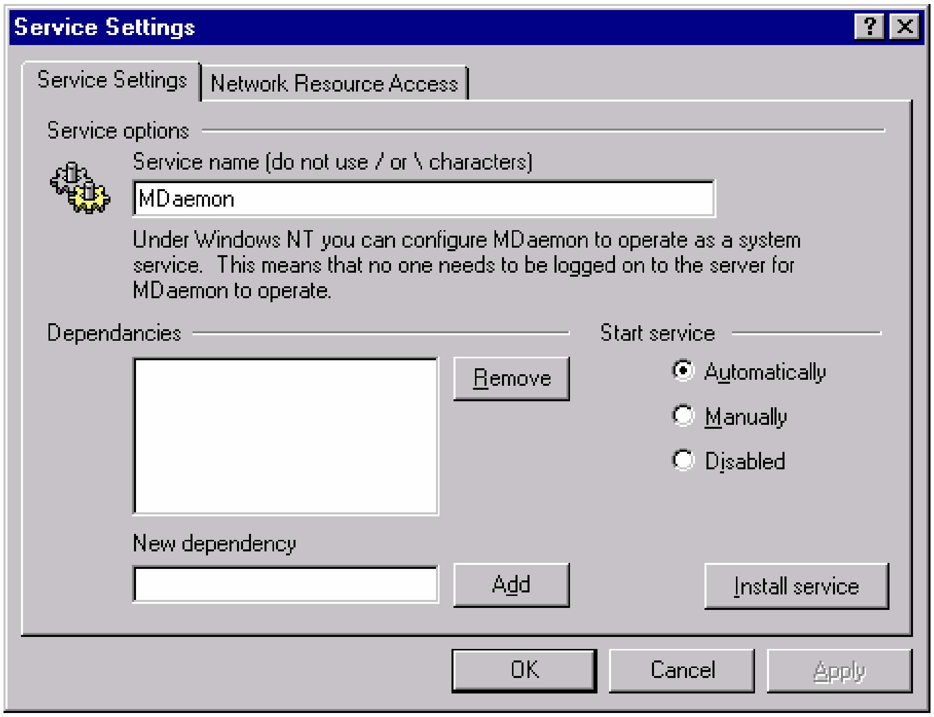
Chapter 17

System Service Settings

Running MDaemon as a System Service.

Use the **Setup | System Service Settings…** menu selection to run MDaemon as a system service under Windows NT/2000 or Windows 9x/ME. MDaemon will detect if you are running Windows 9x and present a different Service Setup Dialog if you are. Although much less sophisticated than under NT/2000, services in Windows 9x will still allow you to operate the software without anyone being logged in.

Service Settings



Service name (do not use / or \ characters): MDaemon

Under Windows NT you can configure MDaemon to operate as a system service. This means that no one needs to be logged on to the server for MDaemon to operate.

Start service
● Automatically
○ Manually
○ Disabled

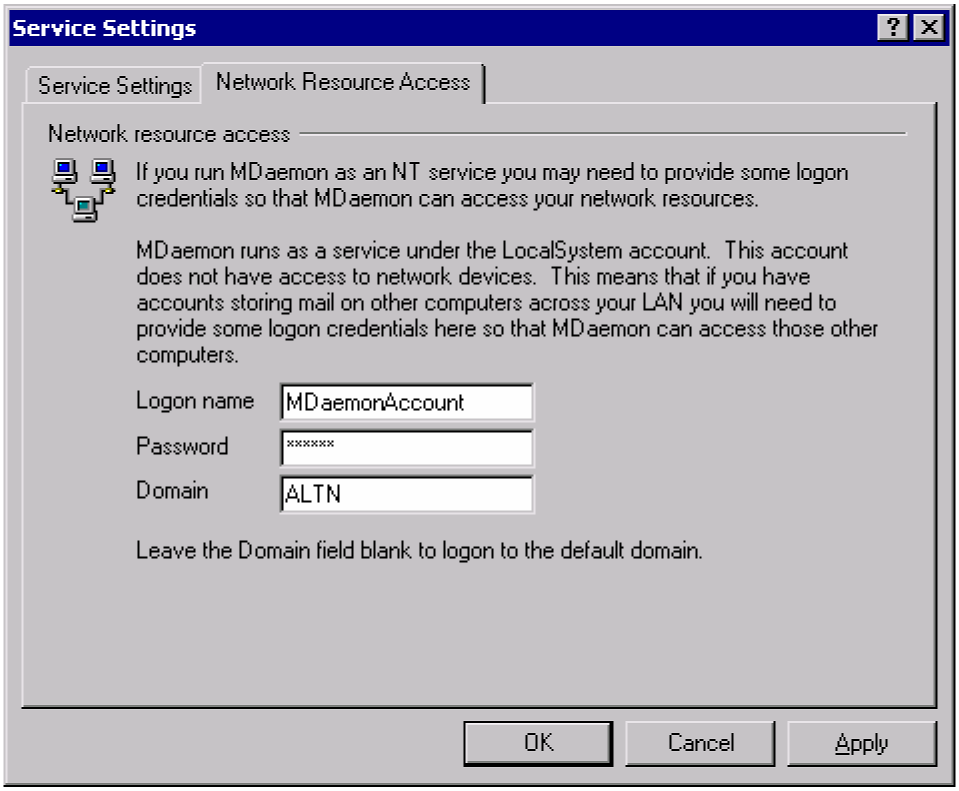
Service Options

Service name
This is the name that NT will use for the service.

Start service
This is the initial state of the service.

Dependencies
A list of Services that must be active **before** the MDaemon service should attempt to load.

Network Resource Access



If you run MDaemon as an NT service you may need to provide some logon credentials so that MDaemon can access your network resources.

MDaemon runs as a service under the LocalSystem account. This account does not have access to network devices. This means that if you have accounts storing mail on other computers across your LAN you will need to provide some logon credentials here so that MDaemon can access those other computers.

Logon name: MDaemonAccount

Password: ******

Domain: ALTN

Leave the Domain field blank to logon to the default domain.

When running MDaemon as an NT/2000 system service, by default it runs under the LocalSystem account. Because this account does not have access to network devices, MDaemon will not be able to access mail if you wish to store it on other computers across your LAN. That is, not unless you provide logon credentials for an account that can be used to provide the MDaemon service access to network shares. We recommend creating a user account specifically designed for running MDaemon with whatever restrictions that you desire, but which has access to those network shares that you want MDaemon to be able to use. That way you can access network shares with UNC notation or mapped drives when running MDaemon as a service. Further, all applications launched by MDaemon (e.g. MDStats and Pre-Processing utilities) will also use the security context of this same NT Account.

Logon name
This is the logon name of the NT Account under which the MDaemon service should run.

Password
This is the NT Account's password.

Domain
This is the NT Domain on which the account resides. Leave this field blank to logon to the default domain.

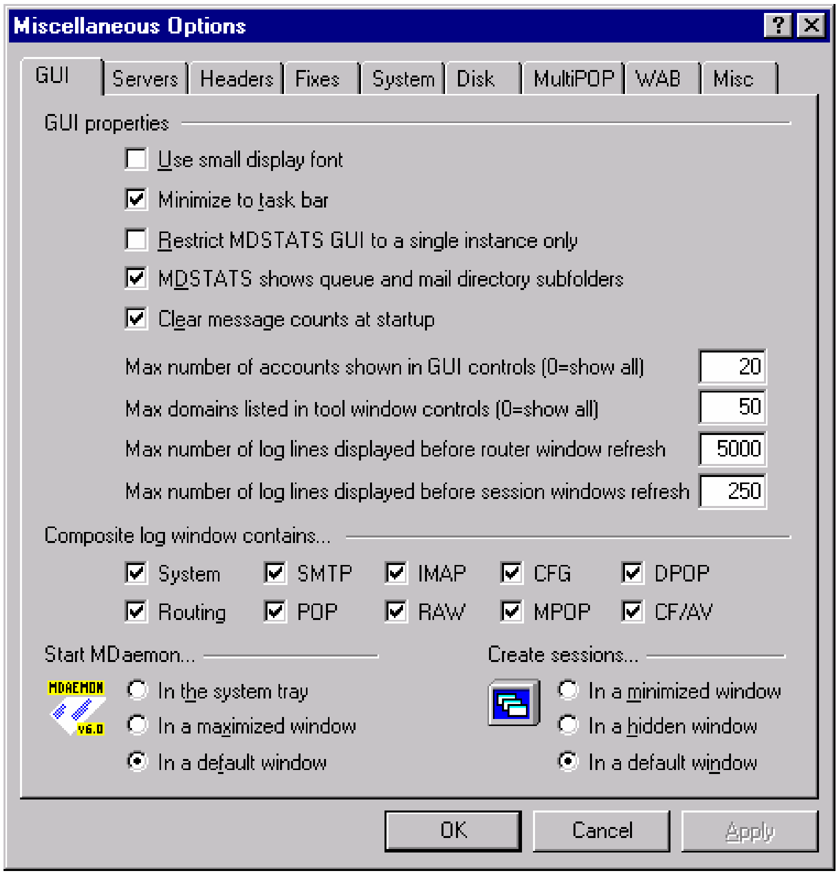
Chapter 18

Miscellaneous Options

MDaemon's Miscellaneous Options settings.

Use the **Setup|Miscellaneous Options…** menu selection to edit various global toggles, set SMTP message size limitations, configure Disk Space Monitoring, and specify default window sizes for Server startup and Mail Sessions.

GUI



GUI properties

☐ Use small display font

☑ Minimize to task bar

☐ Restrict MDSTATS GUI to a single instance only

☑ MDSTATS shows queue and mail directory subfolders

☑ Clear message counts at startup

Max number of accounts shown in GUI controls (0=show all) 20

Max domains listed in tool window controls (0=show all) 50

Max number of log lines displayed before router window refresh 5000

Max number of log lines displayed before session windows refresh 250

Composite log window contains...

☑ System ☑ SMTP ☑ IMAP ☑ CFG ☑ DPOP

☑ Routing ☑ POP ☑ RAW ☑ MPOP ☑ CF/AV

Start MDaemon...

○ In the system tray

○ In a maximized window

● In a default window

Create sessions...

○ In a minimized window

○ In a hidden window

● In a default window

Note

The controls on this tab do not affect the amount of data that is actually stored in the log files – they only affect the information displayed in the router window of MDaemon's main interface.

GUI Properties

Use small display font on router & session windows
Enables the small display font on the Router and Session windows.

Clear message counts at startup
When this checkbox is enabled, the message statistics information displayed on the main router window will be reset whenever MDaemon is launched.

Minimize to task bar
When this control is enabled and MDaemon is minimized, it will appear on both the taskbar and in the system tray. Clear this checkbox if you do not want MDaemon to appear on the Windows taskbar when the program is minimized; only the tray icon will be visible.

Restrict MDStats GUI to a single instance only
Click this checkbox if you do not want more the one copy of MDaemon's queue and statistics manager to be able to run at once. Attempting to launch MDStats when it is already running will simply cause the currently running instance to become the active window.

MDStats shows queue and mail directory subfolders
Click this checkbox if you want the queue statistics manager to display subfolders contained in the various queues and user mail directories.

Max number of accounts shown in GUI controls (0=show all)
This is the maximum number of accounts that will be shown in the drop-down list boxes on various dialogs. Further, when the value in this control is set to anything other than "0" (show all) the "Edit Account" and "Delete Account" options will no longer appear on the Accounts menu. Those functions will only be available from the Accounts Manager. You must restart MDaemon before any changes to this control will go into effect.

Max domains listed in tool window controls (0=show all)
This is the maximum number of secondary domains that will be listed under the "Servers" controls in the main display's tool window. After changing this value, you must press F5 or restart MDaemon before the change will be visible in the tool window. This control cannot be set to anything less than 50.

Max number of log lines displayed before router window refresh
This is the maximum number of lines that will be displayed in the log window of the main display. When this number of lines is reached the window will be cleared. This has no affect on the log file. Only the display will be cleared.

Max number of log lines displayed before session windows refresh
This is the maximum number of lines that will appear in each session Connection window before it is cleared. This has no affect on the log file.

Composite log window contains…

Located on the Windows menu of MDaemon's menu bar is a Composite log view option. Clicking that option will add a window to the router that will combine the information displayed on one or more of the router's tabs. Use the controls in this section to designate which tabs' information to combine in that window. The information contained on the following tabs can be combined:

System – Displays MDaemon's system activity such as initializing services and enabling/disabling any of MDaemon's various servers.

SMTP – All send/receive session activity using the SMTP protocol is displayed on this tab.

IMAP – Mail sessions using the IMAP protocol are logged on this tab.

CFG – All MDConfig activity is displayed on the CFG tab.

DPOP – This tab displays MDaemon's DomainPOP activity.

Routing – Displays the routing information (To, From, Message ID, and so on) for each message that is parsed by MDaemon.

POP – When users collect email from MDaemon using the POP3 protocol, that activity is logged here.

RAW – RAW or system generated message activity is logged on this tab.

MPOP – This tab displays MDaemon's MultiPOP mail collection activities.

CF/AV – MDaemon's Content Filter and AntiVirus operations are listed on this tab.

Start MDaemon…

In the system tray
Choose this option if you want MDaemon's interface to be minimized at startup.

In a maximized window
Choose this option if you want MDaemon's interface to be maximized at startup.

In a default window
Choose this option if you want MDaemon's interface to appear in a default window at startup.

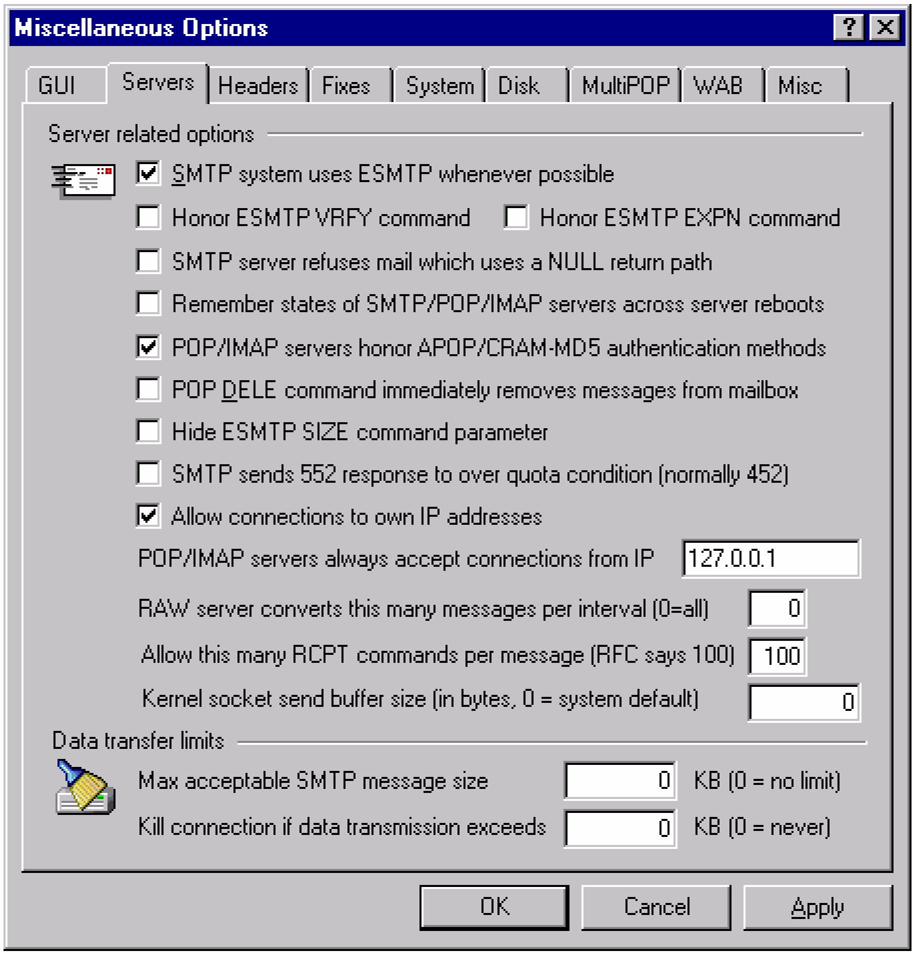
Create Session…

In a minimized window
If this option is selected MDaemon will create new mail session windows in a minimized state.

In a hidden window
If this options is selected MDaemon will create new mail session windows that are completely hidden from view.

In a default window
If this option is selected MDaemon will create new mail session windows using the default settings provided by Windows which relate to size and visibility.

Servers



Server related options

☑ SMTP system uses ESMTP whenever possible

□ Honor ESMTP VRFY command □ Honor ESMTP EXPN command

□ SMTP server refuses mail which uses a NULL return path

□ Remember states of SMTP/POP/IMAP servers across server reboots

☑ POP/IMAP servers honor APOP/CRAM-MD5 authentication methods

□ POP DELE command immediately removes messages from mailbox

□ Hide ESMTP SIZE command parameter

□ SMTP sends 552 response to over quota condition (normally 452)

☑ Allow connections to own IP addresses

POP/IMAP servers always accept connections from IP 127.0.0.1

RAW server converts this many messages per interval (0=all) 0

Allow this many RCPT commands per message (RFC says 100) 100

Kernel socket send buffer size (in bytes, 0 = system default) 0

Data transfer limits

Max acceptable SMTP message size 0 KB (0 = no limit)

Kill connection if data transmission exceeds 0 KB (0 = never)

Server Related Options

SMTP system uses ESMTP whenever possible
Select this switch if you wish to enable support for extended SMTP commands.

Honor ESMTP VRFY commands
Click this switch to allow ESMTP VRFY commands.

Honor ESMTP EXPN commands
Click this checkbox if you want MDaemon to honor ESMTP EXPN commands.

SMTP server refuses mail which uses a NULL return path (RFC no-no)
Click this checkbox if you want the SMTP server to refuse mail that uses a `NULL` return path.

Remember states of SMTP/POP/IMAP servers across server reboots
If this control is enabled, MDaemon will ensure that the state of its servers (enabled or disabled) remains the same after a reboot.

POP/IMAP servers honor APOP/CRAM-MD5 authentication methods

Enable this control if you want MDaemon's POP and IMAP servers to honor the APOP and CRAM-MD5 methods of authentication. These methods provide extra security by making it possible for users to be authenticated without sending clear text passwords.

POP DELE command immediately removes messages from mailbox
Click this switch and MDaemon will delete immediately messages that a user has retrieved even if the POP session does not complete properly.

Hide ESMTP SIZE command parameter
Click this checkbox if you want the ESMTP SIZE command parameter to be hidden.

SMTP sends 552 response to over quota condition (normally 452)
Enabling this control will cause a 552 response ("Requested mail action aborted: exceeded storage allocation") when delivery is attempted to a recipient whose account exceeds its quota. Normally there would be a 452 response ("Requested action not taken: insufficient system storage").

POP/IMAP servers always accept connections from IP [IP address]
The POP and IMAP servers will always accept connections from the IP Address entered into this field regardless of screening and shielding settings.

RAW server converts this many messages per interval
Use this control if you wish to limit the number of RAW messages that may be converted during any given mail processing interval. If the limit is reached then MDaemon will wait until the next processing interval before converting further messages.

Allow this many RCPT commands per message (RFC says 100)
Use this control if you wish to limit the number of RCPT commands that can be sent per message.

Kernel socket send buffer size (in bytes, 0=system default)
If you wish to designate a non system-default socket send buffer size then you can use this control to do so. Specify the new size (in bytes) in the space provided.

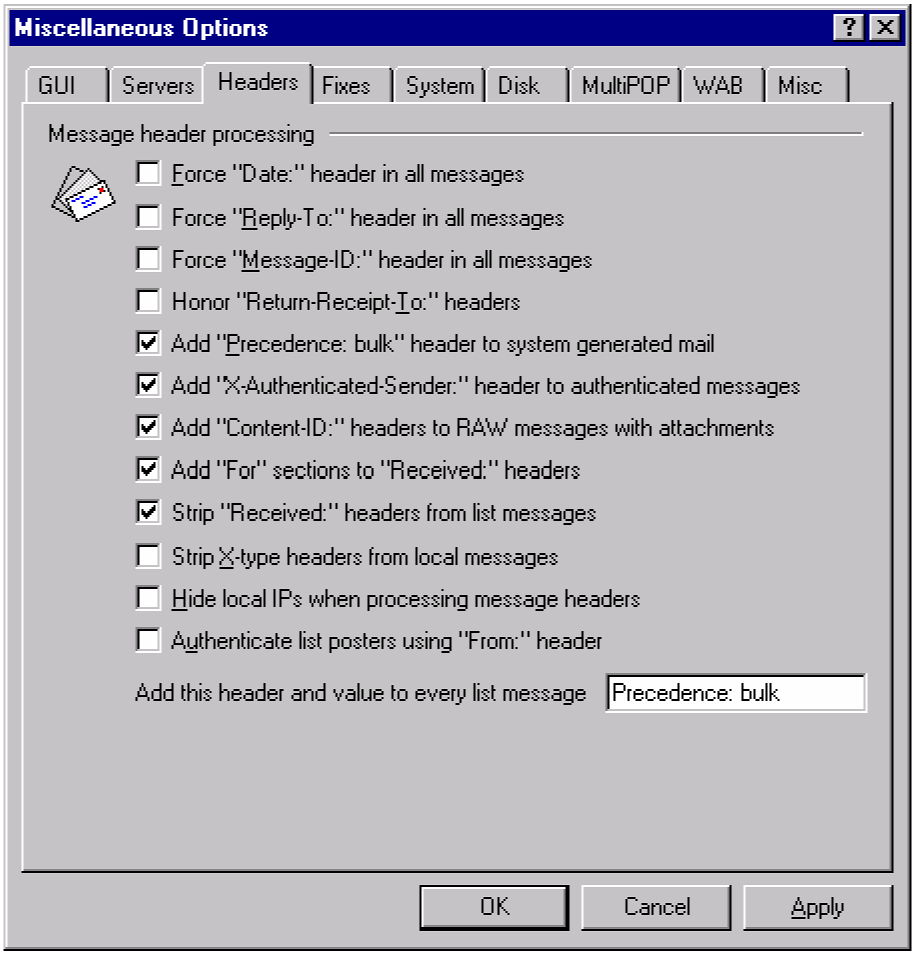
Data Transfer Limits

Max acceptable SMTP message size
Setting a value here will prevent MDaemon from accepting or processing SMTP delivered mail that exceeds a certain fixed size. When this feature is active MDaemon will attempt to use the ESMTP SIZE command specified in RFC-1870. If the sending agent supports this SMTP extension then MDaemon will determine the message size prior to its actual delivery and will refuse the message instantly. If the sending agent does not support this SMTP extension then MDaemon will have to begin acceptance of the message, track its size periodically during transfer, and finally refuse to deliver the message once the transaction has completed.

Kill connection if data transmission exceeds XX KB
If the transmission of data during an MDaemon connection exceeds this threshold, MDaemon will close the connection.

=

Headers



Message header processing

☐ Force "Date:" header in all messages

☐ Force "Reply-To:" header in all messages

☐ Force "Message-ID:" header in all messages

☐ Honor "Return-Receipt-To:" headers

☑ Add "Precedence: bulk" header to system generated mail

☑ Add "X-Authenticated-Sender:" header to authenticated messages

☑ Add "Content-ID:" headers to RAW messages with attachments

☑ Add "For" sections to "Received:" headers

☑ Strip "Received:" headers from list messages

☐ Strip X-type headers from local messages

☐ Hide local IPs when processing message headers

☐ Authenticate list posters using "From:" header

Add this header and value to every list message: Precedence: bulk

Message Header Processing

Force "Date" header in all messages

When a message is encountered which doesn't have a "`Date:`" header, MDaemon will create one and add it to the message file if this switch is selected. It will be the date on which MDaemon first receives the message, not when it was created by a mail client. There are some mail clients that do not create this header, and since some mail servers refuse to honor such messages this feature will enable them to be delivered.

Force "Reply-To" header in all messages

When a message is encountered which doesn't have a "`Reply-To`" header, MDaemon will create and add one to the message file using the address found in the "`From`" header. If a "`Reply-To`" header is present but **empty**, MDaemon will create the header like this: `Reply-To:` "". This fixes problems for some mail clients.

Force "Message-ID" header in all messages

When a message is encountered which doesn't have a "`Message-ID`" header, MDaemon will create one at random and insert it into the message.

Honor "Return-Receipt-To" headers

This switch determines how MDaemon will behave when faced with a request for deliver confirmation from an incoming message. If set, a confirmation message will be dispatched to the sender of the triggering message. Otherwise such requests are ignored.

Add "Precedence: bulk" header to system generated mail
Click this option if you want all system generated messages (welcome messages, warnings, "could not deliver" messages, and so on) to have a "Precedence: bulk" header inserted.

Add "X-Authenticated-Sender:" header to authenticated messages
Check this switch if you want MDaemon to add an "X-Authenticated-Sender:" header to messages that arrive on an authenticated session using the `AUTH` command.

Add "Content-ID:" headers to RAW messages with attachments
Click this switch if you wish to add unique MIME `Content-ID` headers to messages that MDaemon creates from a RAW file that contains attachments.

Add "For" sections to "Received:" headers
Click this switch if you want "`For` [SMTP Recipient]" sections to be added to the message's "`Received:`" header added by MDaemon.

Strip "Received:" headers from list messages
Click this switch if you wish to strip all existing "`Received:`" headers from list messages. This is sometimes useful for Mailing List mail.

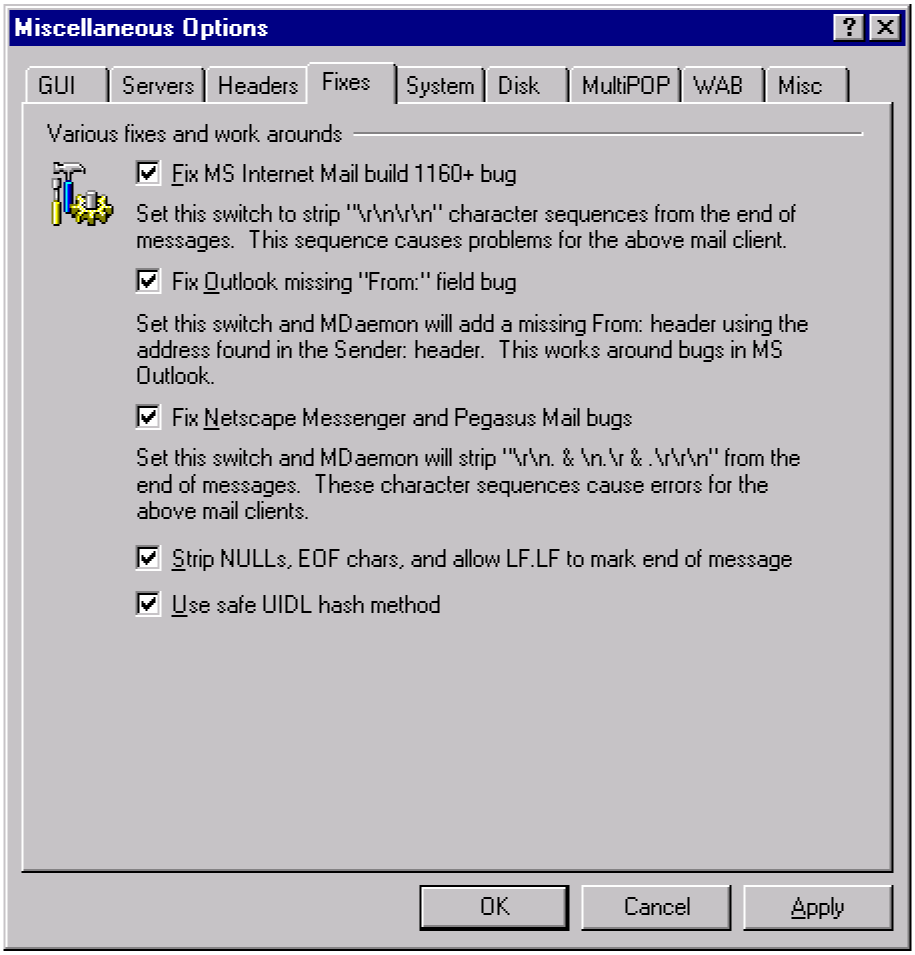
Strip X-type headers from local messages
MDaemon uses many server specific headers called `X-Type` headers in order to route mail and perform various MDaemon specific functions. This switch will force MD to clean up after itself and remove these headers from messages as they are moved into local mailboxes.

Hide local IPs when processing message headers
Click this option to prevent MDaemon from placing local IP addresses into message headers when it processes mail.

Authenticate list posters using "From:" header
Usually senders to private lists are checked using the `MAIL FROM` value passed during the SMTP session. If you would rather have your system use the message's "`FROM:`" header then enable this switch.

Add this header and value to every list message [`header`]
If you wish to add a static header/value combination (such as "Precedence: bulk") to all list messages, then specify it here.

Fixes



Various fixes and work arounds

☑ Fix MS Internet Mail build 1160+ bug

Set this switch to strip "\r\n\r\n" character sequences from the end of messages. This sequence causes problems for the above mail client.

☑ Fix Outlook missing "From:" field bug

Set this switch and MDaemon will add a missing From: header using the address found in the Sender: header. This works around bugs in MS Outlook.

☑ Fix Netscape Messenger and Pegasus Mail bugs

Set this switch and MDaemon will strip "\r\n. & \n.\r & .\r\r\n" from the end of messages. These character sequences cause errors for the above mail clients.

☑ Strip NULLs, EOF chars, and allow LF.LF to mark end of message

☑ Use safe UIDL hash method

Various Fixes and Work Arounds

Fix MS Internet mail build 1160+ bug

This switch has been added in an attempt to deal with the Microsoft Internet Mail problem of messages not appearing on the display after they are downloaded. With this switch turned on, MDaemon will strip consecutive `CRLFCRLF` sequences from the end of the message body. Three sets of `CRLF` pairs at the tail end of a message file is the cause of the Microsoft problem.

Fix MS Outlook missing "from" field bug

Some versions of Microsoft Outlook fail to create a FROM header when you compose a message. The `FROM` field information is instead placed in the SENDER field. This can confuse downstream mail servers as well as the recipient of your message. Select this switch and MDaemon will create the missing `FROM` field using the address found in the `SENDER` field.

Fix Netscape Messenger and Pegasus Mail bugs

This switch adds support for correcting three bugs present in various versions of Netscape Messenger and Pegasus Mail. Without this switch set messages collected with those clients have the potential to be mishandled by them. When the option is checked `\r\n.`, `\n.\r`, and `.\r\r\n` will be stripped from the end of messages.

Strip NULLs, EOF chars, and allow LF.LF to mark end of message

Allow `Nulls`, EOF characters, and `LF.LF` for end of message mark in addition to the normal `CRLF.CRLF` sequence.

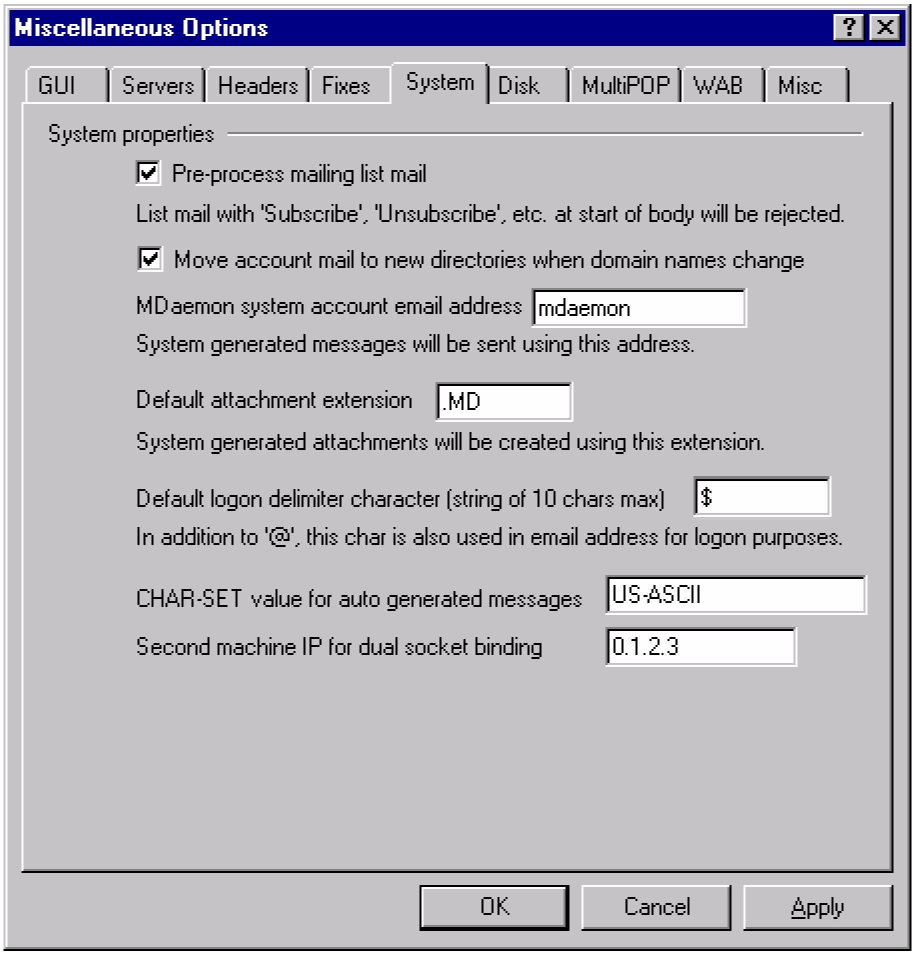
Use safe UIDL hash method

When you have configured MDaemon to leave messages on the host server after it has downloaded them, a UIDL hash method is used to identify those already retrieved messages. Previously MDaemon's UIDL hash method was not compatible with Windows' treatment of Daylight Savings Time. All stored messages would appear to be new and thus downloaded again a single time. Enable this feature if you want to switch to the new "safe" UIDL hash method that is unaffected by Daylight Savings Time.

Note

Switching to the new hash method will cause all stored messages to appear to be new a single time and thus downloaded again. Thereafter messages will be unaffected by Daylight Savings Time.

System



System properties

☑ Pre-process mailing list mail

List mail with 'Subscribe', 'Unsubscribe', etc. at start of body will be rejected.

☑ Move account mail to new directories when domain names change

MDaemon system account email address: mdaemon

System generated messages will be sent using this address.

Default attachment extension: .MD

System generated attachments will be created using this extension.

Default logon delimiter character (string of 10 chars max): $

In addition to '@', this char is also used in email address for logon purposes.

CHAR-SET value for auto generated messages: US-ASCII

Second machine IP for dual socket binding: 0.1.2.3

System Properties

Pre-process mailing list mail

When a message arrives for a mailing list that should have been directed to the system address, MDaemon will reject it when this control is enabled. For example, a user may join or leave a list by placing the Subscribe or Unsubscribe command at the beginning of an email message and sending it to the system address. Oftentimes users erroneously try to send these messages to the list itself. Enabling this control will prevent these messages from being posted to the list.

Move account mail to new directories when domain names change

If this checkbox is enabled when you rename a domain, that domain's existing account mail will be moved to directories with the new name. Otherwise, MDaemon will continue to use the old mail directory names.

MDaemon system account email address [address]

This is the email address from which system generated messages will come. Subscription confirmations, "Could not deliver" messages, various notification messages, and so on are all system messages.

Default attachment extension

System generated messages will be created using this extension. This will also be the extension assigned to attachments included with system generated messages. For example, if MDaemon generates a warning message to the postmaster about a specific message it will attach that message with an extension of ".md".

Default logon delimiter character (string of 10 characters max)

When using an email address as the account logon parameter, this character or string of characters can be used as an alternative to "@". This may be necessary for some users that have email clients which do not support "@" in the logon field. For example, if you used "$" in this field then users could login using "user@domain.com" or "user$domain.com".

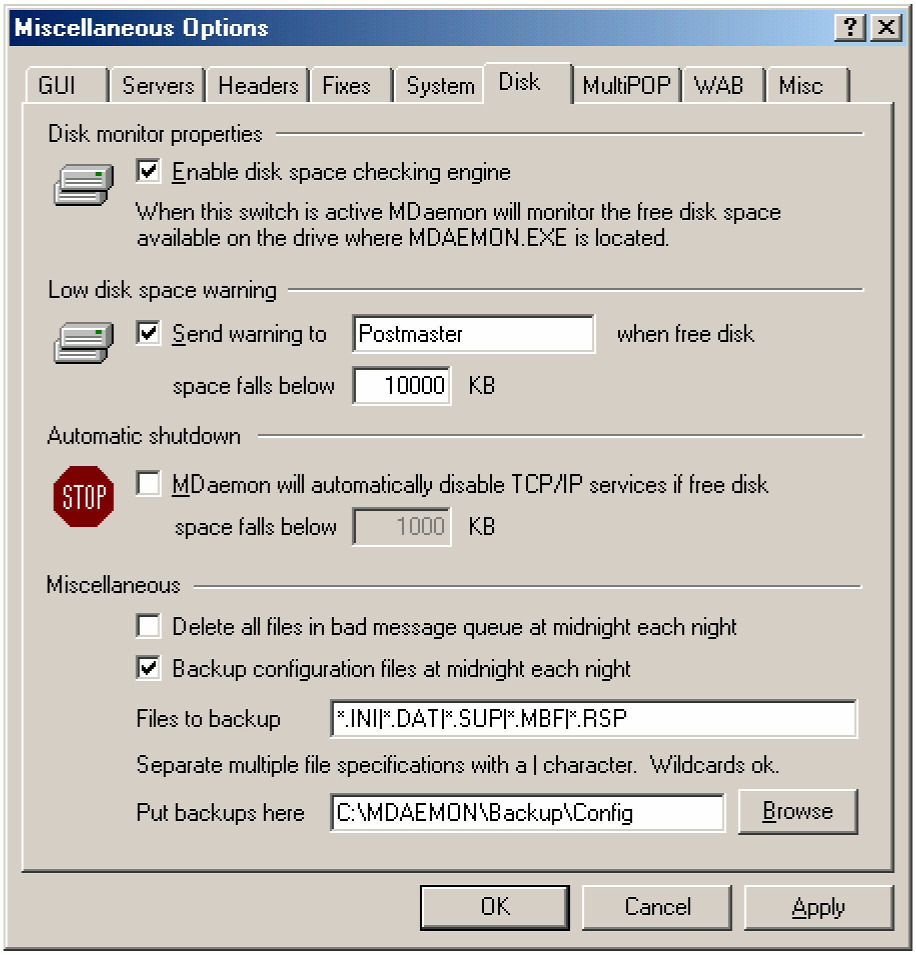
CHAR-SET value for auto-generated messages

Specify the character set that you wish to be used for auto-generated messages. The default setting is US-ASCII.

Second machine IP for dual socket binding

If you want the Primary domain to be bound to an additional IP address then include it here.

Disk



Disk monitor properties

☑ Enable disk space checking engine

When this switch is active MDaemon will monitor the free disk space available on the drive where MDAEMON.EXE is located.

Low disk space warning

☑ Send warning to Postmaster when free disk space falls below 10000 KB

Automatic shutdown

☐ MDaemon will automatically disable TCP/IP services if free disk space falls below 1000 KB

Miscellaneous

☐ Delete all files in bad message queue at midnight each night

☑ Backup configuration files at midnight each night

Files to backup: *.INI|*.DAT|*.SUP|*.MBF|*.RSP

Separate multiple file specifications with a | character. Wildcards ok.

Put backups here: C:\MDAEMON\Backup\Config

Disk Monitor Properties

Enable disk space checking engine

Activate this checkbox if you want MDaemon to monitor the amount of disk space that is available on the drive where the MDAEMON.EXE is located.

Low Disk Space Warning

Send warning to [user or address] when free disk space falls below [xx] KB

By using this option you can configure MDaemon to send a notification message to the user or address of your choice when disk space drops below a certain level.

Automatic Shutdown

MDaemon will automatically disable TCP/IP services if free disk space falls below [xx] KB

Enable this feature if you want MDaemon to disable TCP/IP Services if free disk space drops to a certain level.

Miscellaneous

Delete all files in bad message queue at midnight each night

Click this checkbox if you want MDaemon to delete all files from the bad message queue each night at midnight. This can help to conserve disk space.

Backup configuration files at midnight each night

Click this checkbox if you want to archive all MDaemon configuration files at midnight each night.

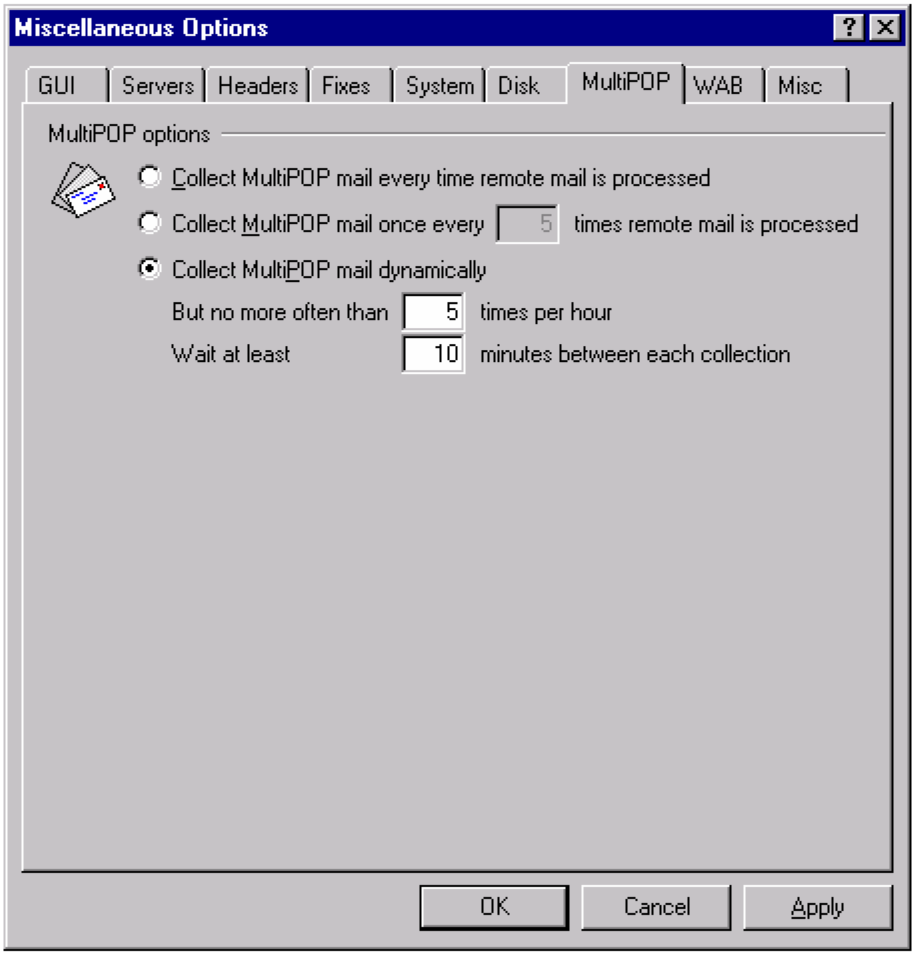
Files to backup

Use this text box to specify exactly which files and file extensions to back up. Wildcards are permitted and each filename or extension must be separated be the "|" character.

Put backups here

Use this control to specify the folder in which you wish the backup files to be stored.

MultiPOP



Miscellaneous Options

MultiPOP options

○ Collect MultiPOP mail every time remote mail is processed

○ Collect MultiPOP mail once every 5 times remote mail is processed

● Collect MultiPOP mail dynamically

But no more often than 5 times per hour

Wait at least 10 minutes between each collection

MultiPOP Collection Frequency

Collect MultiPOP mail every time remote mail is processed

Click this option if you want MDaemon to collect all MultiPOP mail every time that remote mail is processed.

Collect MultiPOP mail once every XX times remote mail is processed

Click this option button and specify a numeral in the box if you want MultiPOP mail to be collected less often than remote mail is processed. The numeral denotes how many times remote mail will be processed before MultiPOP mail will be collected.

Collect MultiPOP mail dynamically

Click this checkbox if you wish to collect MultiPOP messages dynamically. Ordinarily, MuliPOP is collected for all users at the same time at each remote mail processing interval, or at every *x* number of intervals. When collected dynamically, MultiPOP messages are collected for each individual user when that user checks his or her local mail via POP, IMAP, or WorldClient rather than for all users at once. However, because MultiPOP collection is triggered by a user checking his email, any new MultiPOP messages collected will not be visible to the user until he checks his mail *again*. Thus, he would need to check his mail twice in order to see new MultiPOP messages – once to trigger MultiPOP and a second time to see the mail that was collected.

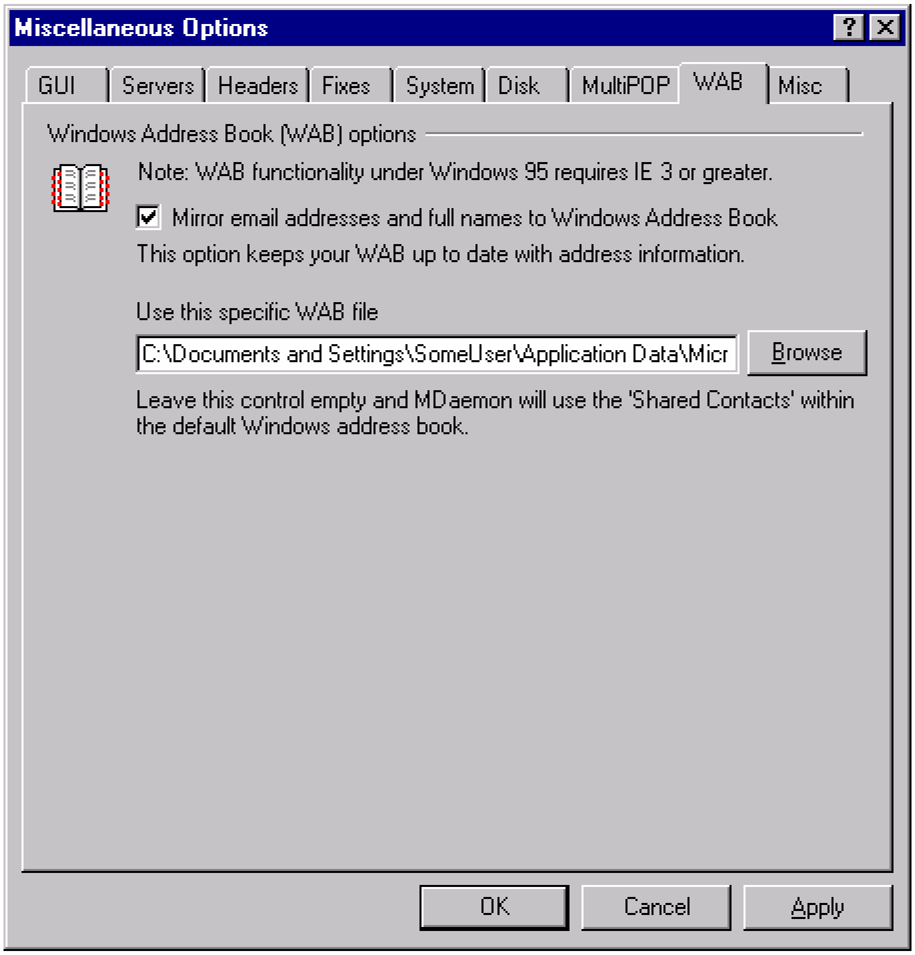
But no more often than XX times per hour

In order to reduce the load that extensive use of MultiPOP can potentially place on your MDaemon, you can use this control to specify a maximum number of times per hour that MultiPOP can be collected for each user.

Wait at least XX minutes between each collection

This option can help to reduce the load on the mail server by limiting how frequently MultiPOP messages can be collected by each user. It will restrict MultiPOP mail collection to once every so many minutes per user. Specify the number of minutes that you wish to require the user to wait before being allowed to check MultiPOP again.

WAB



Windows Address Book (WAB) options

Note: WAB functionality under Windows 95 requires IE 3 or greater.

☑ Mirror email addresses and full names to Windows Address Book

This option keeps your WAB up to date with address information.

Use this specific WAB file

C:\Documents and Settings\SomeUser\Application Data\Micr

Leave this control empty and MDaemon will use the 'Shared Contacts' within the default Windows address book.

MDaemon version 6 has the ability to automatically keep a Windows Address Book file (*.wab) or Microsoft Outlook Contact Store current with each account's full name and email address. This is desirable for those who wish to share an address book among users of products like Outlook, but do not wish to use an LDAP server for that purpose.

Windows Address Book (WAB) Options

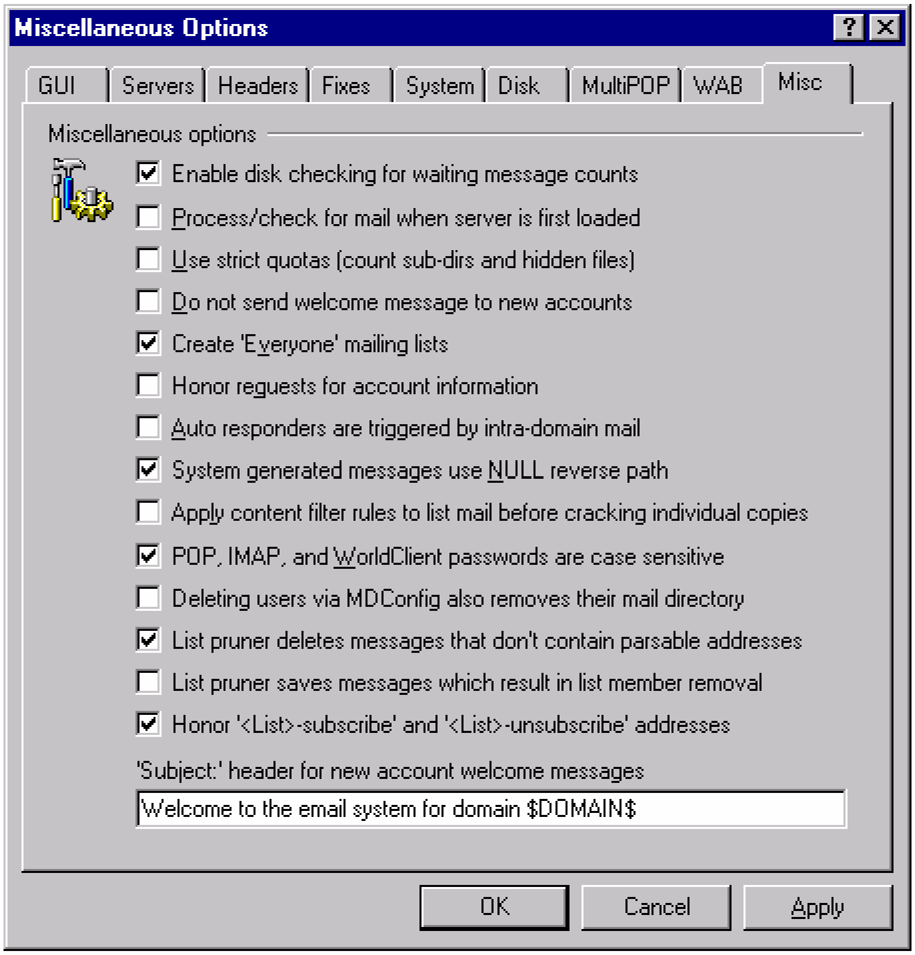
Mirror email addresses and full names to Windows Address Book

Enable this checkbox if you want your users' names and email addresses to be mirrored to a *.wab file or the Microsoft Outlook Contact Store. In the Windows Address Book, on the Tools|Options menu, you can configure whether or not your Windows Address Book will share contact information between Outlook and other applications by storing data in the Microsoft Outlook Contact Store or an address book (*.wab) file.

Use this specific WAB file

Specify the path to the *.wab file in which you wish to mirror your user information. If you leave this control empty then MDaemon will use the shared contacts store within the default Windows Address Book.

Misc



Miscellaneous options

☑ Enable disk checking for waiting message counts

□ Process/check for mail when server is first loaded

□ Use strict quotas (count sub-dirs and hidden files)

□ Do not send welcome message to new accounts

☑ Create 'Everyone' mailing lists

□ Honor requests for account information

□ Auto responders are triggered by intra-domain mail

☑ System generated messages use NULL reverse path

□ Apply content filter rules to list mail before cracking individual copies

☑ POP, IMAP, and WorldClient passwords are case sensitive

□ Deleting users via MDConfig also removes their mail directory

☑ List pruner deletes messages that don't contain parsable addresses

□ List pruner saves messages which result in list member removal

☑ Honor '<List>-subscribe' and '<List>-unsubscribe' addresses

'Subject:' header for new account welcome messages

Welcome to the email system for domain $DOMAIN$

Enable disk checking for waiting message counts

This switch governs whether MDaemon will check the disk to count waiting messages in the mail queues. Doing so can cause excessive disk spin over the long term.

Process/check for mail when server is first loaded

If selected MDaemon will create a mail processing event when it first loads.

Use strict quotas (count subdirectories and hidden files)

When this box is checked, all files and subdirectories will apply toward any size or message number limitations placed on a user's account mailbox. Otherwise, only actual message files will count toward these limitations.

Do not send welcome message to new accounts

By default, MDaemon will generate a Welcome message based upon the `welcome.dat` file and distribute it to new users when their account is created. Enable this control if you want to prevent the message from being generated.

Create "Everyone" mailing lists

Clear this checkbox if you do not wish "Everyone" mailing lists to be created and maintained for your domains. Maintaining mailing lists of every user on every MDaemon domain could be a potential waste of resources if the lists are never used or are for very large numbers of users. Clear this checkbox if you do not want MDaemon create these lists.

Honor requests for account information
Provides the user list when requested via EXPN or LISTS commands.

Auto responders are triggered by local as well as remote mail
Sometimes it is advantageous to disable the auto-response engine for local mail traffic.

System generated messages use NULL reverse path
Click this checkbox if you want auto-generated emails to be sent with a NULL reverse path. This switch is checked by default in order to comply with SMTP email standards, but in spite of these standards some servers refuse to accept emails which are generated with a NULL reverse path, so you can clear this switch if you desire. However, in some cases (such as auto-responders for example) using anything other than a NULL reverse path can lead to mail loops.

Apply content filter rules to list mail before individual messages for list members are cracked
When the *MDaemon will crack list mail* option is chosen on the Routing tab of the mailing list editor, enabling this control will cause the content filter rules to be applied to list messages before they are cracked and distributed to list members.

POP, IMAP, WorldClient passwords are case sensitive
POP, IMAP, and WorldClient passwords will be case-sensitive when this control is checked.

Deleting users via MDConfig also removes their mail directory
Click this checkbox if you want users' mail directories to be deleted when their account is deleted via MDConfig. Otherwise, their account will be deleted but their messages and directories will remain.

List pruner deletes messages that don't contain parsable addresses
When you have configured MDaemon to scan messages that are returned to a Mailing List in an attempt to delete list members that cannot be reached, this control will cause those messages to be deleted that do not contain a parsable address. For more information, see the *Automatically remove dead addresses from list membership* control on the Members tab of the Mailing List editor (page 271).

List pruner saves messages which result in list member removal
When MDaemon scans returned list messages in an attempt to remove member addresses that cannot be reached, this control will cause messages that result in a list member's removal to be saved.

Honor '<List>-subscribe' and '<List>-unsubscribe' addresses
Click this checkbox if you want MDaemon to recognize email addresses of this format as valid (as long as the list actually exists) in order to facilitate an easier method for users to join and leave your mailing lists. For example: suppose you have a list called `MyList@altn.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@altn.com` and `MyList-Unsubscribe@altn.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@domain.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

“Subject” header for new account welcome messages

When MDaemon sends the “Welcome” message to new accounts, this text will appear as the message’s “Subject” header. The welcome message is constructed from the `Welcome.dat` file contained in the …`/MDaemon/app/` directory, and this subject header control may contain any macros permitted in auto response scripts (page 261).

SECTION II

MDAEMON® VERSION 6

MDaemon's Account Features

Chapter

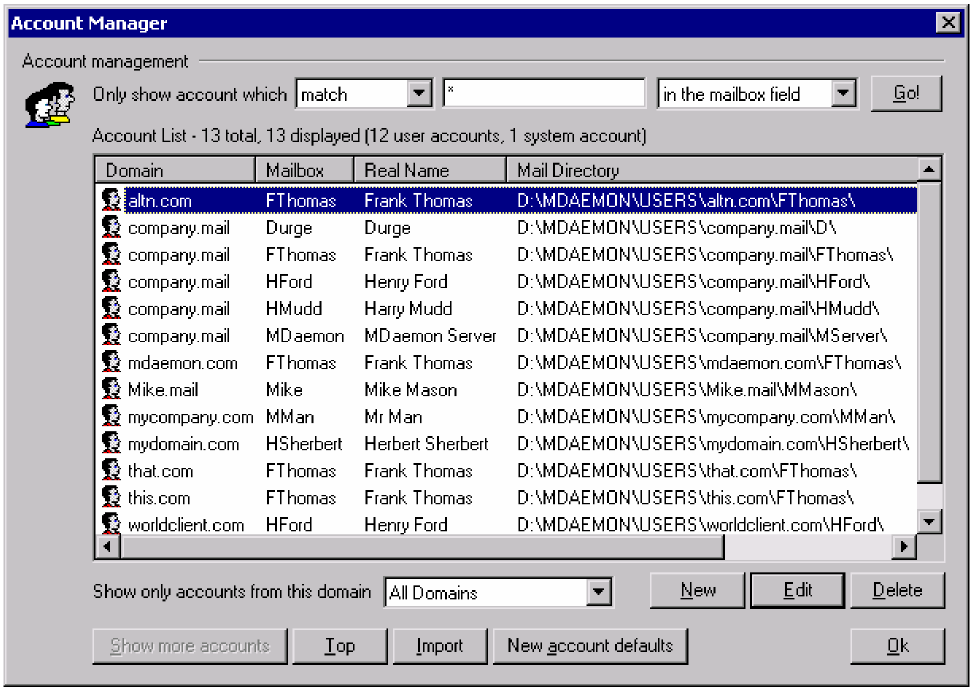
19

Managing MDaemon Accounts

Managing and editing your MDaemon User Accounts.

Account Manager

To better manage the selection, addition, deletion, or modification of your accounts, MDaemon version 6 contains the Account Manager (**Accounts|Account Manager…**). This dialog provides access to account information and can be used to sort accounts by domain, name, or mail directory.



Account Manager

Account management

Only show account which: match | * | in the mailbox field

Account List - 13 total, 13 displayed (12 user accounts, 1 system account)

Domain	Mailbox	Real Name	Mail Directory
altn.com	FThomas	Frank Thomas	D:\MDAEMON\USERS\altn.com\FThomas\
company.mail	Durge	Durge	D:\MDAEMON\USERS\company.mail\D\
company.mail	FThomas	Frank Thomas	D:\MDAEMON\USERS\company.mail\FThomas\
company.mail	HFord	Henry Ford	D:\MDAEMON\USERS\company.mail\HFord\
company.mail	HMudd	Harry Mudd	D:\MDAEMON\USERS\company.mail\HMudd\
company.mail	MDaemon	MDaemon Server	D:\MDAEMON\USERS\company.mail\MServer\
mdaemon.com	FThomas	Frank Thomas	D:\MDAEMON\USERS\mdaemon.com\FThomas\
Mike.mail	Mike	Mike Mason	D:\MDAEMON\USERS\Mike.mail\MMason\
mycompany.com	MMan	Mr Man	D:\MDAEMON\USERS\mycompany.com\MMan\
mydomain.com	HSherbert	Herbert Sherbert	D:\MDAEMON\USERS\mydomain.com\HSherbert\
that.com	FThomas	Frank Thomas	D:\MDAEMON\USERS\that.com\FThomas\
this.com	FThomas	Frank Thomas	D:\MDAEMON\USERS\this.com\FThomas\
worldclient.com	HFord	Henry Ford	D:\MDAEMON\USERS\worldclient.com\HFord\

Show only accounts from this domain: All Domains

Account List

Above the Account List you will see two statistics regarding the list. The first number is the total number of MDaemon user accounts that currently exist on your system. The second number is the number of those accounts currently displayed in the Account List. Which accounts that will be displayed is contingent upon what you have chosen in the *Show Only Accounts From This Domain* control. If you have selected "All Domains" then all of your MDaemon accounts will be displayed in the list.

Each Account List entry lists the Domain to which it belongs, the Mailbox, the "Real Name" of the account holder, and the Mail Directory in which the account's messages are stored. This list can be sorted in ascending and descending order by whichever column that you prefer. Click any column heading to sort the list in ascending order by that column. Click the column again to sort it in descending order.

Note

By default, only 500 accounts at a time will be displayed in this list. If you want to see more accounts from the currently selected domain (or All Domains, if you have selected that option) then you must click the "**Show More Accounts**" button to display the next 500. If you want to be able to display more than 500 accounts at a time then open the `MDaemon.ini` file and change the `MaxAccountManagerEntries=500` key to whatever value that you prefer.

Show only accounts from this domain
Choose "All Domains" from this drop-down list box to display all MDaemon accounts. Choose a specific domain to show only that domain's accounts.

New
Click this button to open the Account Editor in order to create a new account.

Edit
Select an account from the Account List and then click this button to open it in the account editor.

Delete
Select an account from the Account List and then click this button to delete it. You will be asked to confirm you decision to delete the account before MDaemon will proceed.

Show more accounts
The account list will only display 500 accounts at a time. If there are more than 500 accounts in the domain that you have chosen then click this button to display the next 500. See the note above for instructions on how to increase the maximum number of accounts that may be displayed.

Top
Click this button to quickly move to the top of the Account List.

Import
This opens the OPEN dialog from which you can choose a text file to import accounts from. This button is identical to the **Accounts | Import | From a text file…** menu selection.

New account defaults
Click this button to open the New Account Defaults dialog. See page 216 for more information.

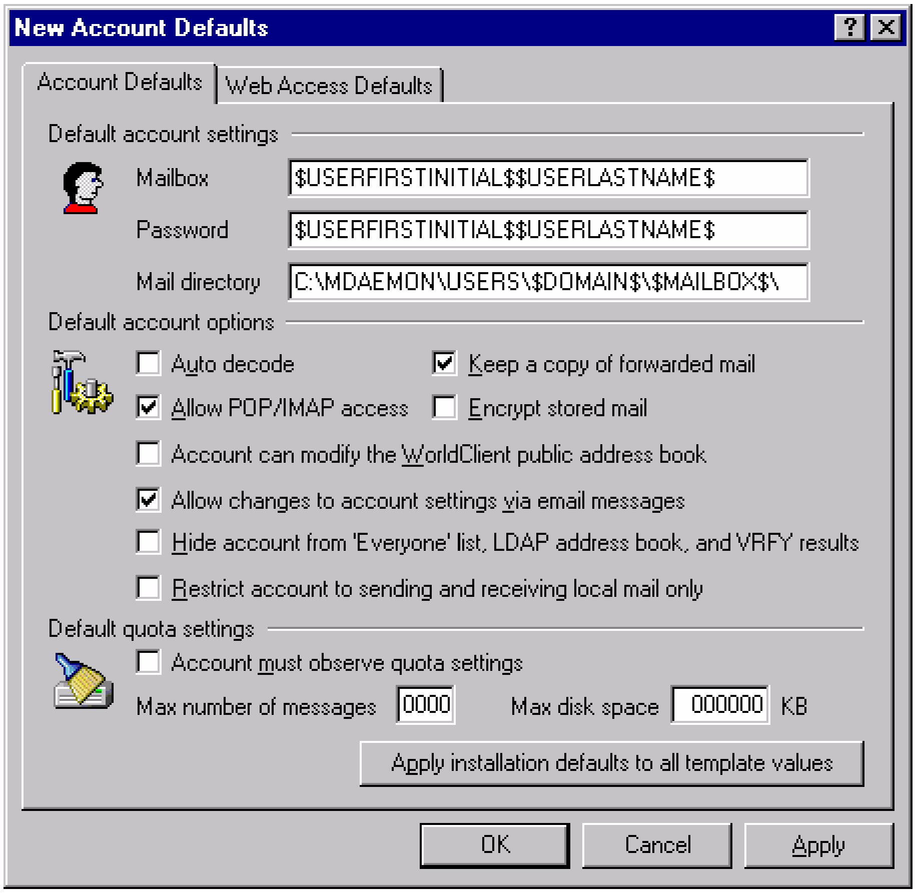
Creating an MDaemon User Account

Create a new MDaemon user account by clicking the new account button on the toolbar or **New** on the Account Manager (page 214). This will open the Account Editor for configuring the account. You can designate default settings for new accounts by using the New Account Defaults dialog (page 216).

New Account Defaults

Use the **Accounts|New Account Defaults…** menu selection to edit your Account Defaults and Web Access Defaults.

Account Defaults



Default account settings

Mailbox: $USERFIRSTINITIAL$$USERLASTNAME$

Password: $USERFIRSTINITIAL$$USERLASTNAME$

Mail directory: C:\MDAEMON\USERS\$DOMAIN$\$MAILBOX$\

Default account options

☐ Auto decode
☑ Keep a copy of forwarded mail
☑ Allow POP/IMAP access
☐ Encrypt stored mail
☐ Account can modify the WorldClient public address book
☑ Allow changes to account settings via email messages
☐ Hide account from 'Everyone' list, LDAP address book, and VRFY results
☐ Restrict account to sending and receiving local mail only

Default quota settings

☐ Account must observe quota settings

Max number of messages: 0000   Max disk space: 000000 KB

Account Defaults contains various account setting controls and template strings. Templates make it possible for you to specify default values for common user account components. The various string values associated with accounts such as *Mailbox* and *POP Password* can be constructed using a variety of special macros that will be replaced by actual values when an account is being created or imported. Use of these templates can greatly simplify and automate new account management.

Default Account Settings

Mailbox

Use this field to specify a default Mailbox name template for new accounts. In addition to being the Mailbox, this value will be the name passed in the `USER` POP command, which enables access to a mailbox from a remote location or POP aware mail clients. See *Macros* below for a list of the Macros that can be used in this template string.

Password

This template specifies a default POP Password for new accounts. This is the value passed in the `PASS` POP command, which allows access to a mailbox from a remote location or POP aware mail clients. See *Macros* below for a list of the Macros that can be used in this template string.

Mail directory

Use this field to specify a default mail directory for new accounts. These directories are where the actual mail files delivered to the mailbox will be stored. Care must be taken to ensure that once expanded, the template provided here will form a true DOS™ path.

Default Account Options

These switches are used for designating default values for various account settings. For more information on these switches, see **Account Editor**—page 222.

Default Quota Settings

These controls are used for designating default values for a new account's quota settings. For more information on these controls, see **Account Editor**—page 222.

Apply Installation Defaults to All Template Values

Clicking this button will cause the controls contained on this tab to be reset to their original installation default settings.

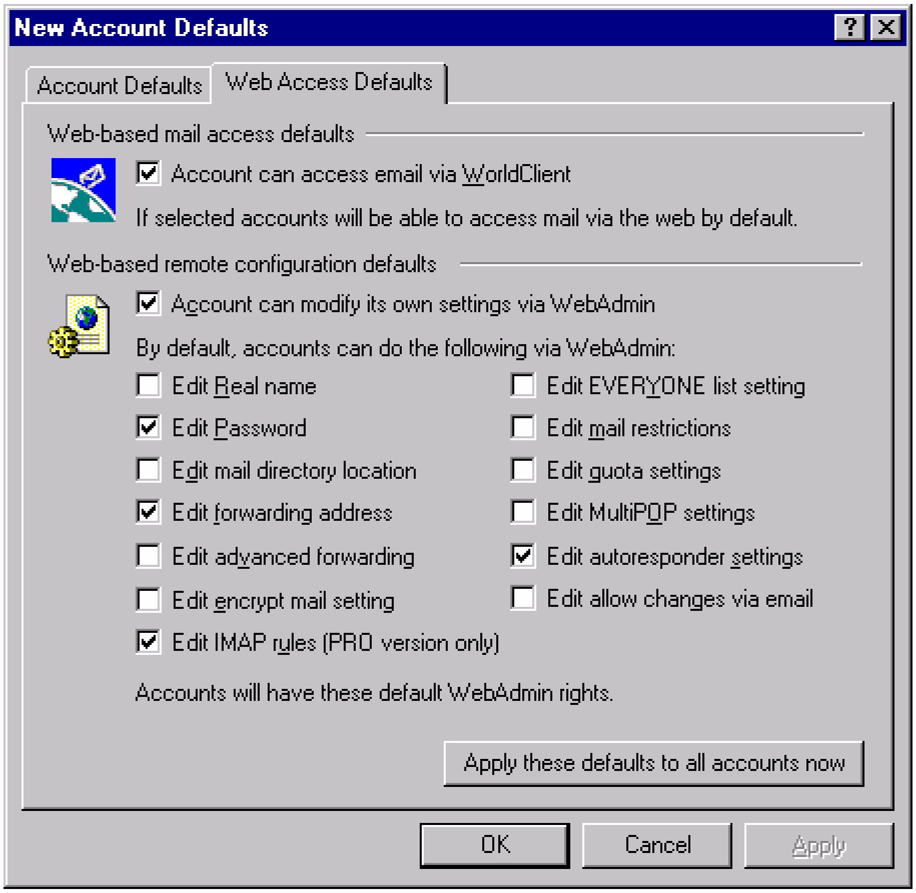
Template Macros

Below is a quick reference to the macros available for automating your account setup.

$DOMAIN$	This variable will resolve to the domain name selected for the account.
$DOMAINIP$	This variable will resolve to the IP associated with the domain currently selected for the account.
$USERNAME$	This variable resolves to the full first and last name of the account holder. This field is equivalent to "$USERFIRSTNAME$ $USERLASTNAME$"
$USERFIRSTNAME$	This variable resolves to the first name of the account holder.
$USERLASTNAME$	This variable resolves to the last name of the account holder.
$USERFIRSTINITIAL$	This variable resolves to the first letter of the account holder's first name.
$USERLASTINITIAL$	This variable resolves to the first letter of the account holder's last name.
$MAILBOX$	This variable resolves to the mailbox name of the current account. The value will also used as the POP user name used in POP3 mail sessions. This is the value expected in the USER command during POP session handshaking.

Web Access Defaults

The Web Access Defaults dialog is used for designating the default access rights that new accounts will have for WorldClient and WebAdmin. You can designate whether or not accounts will be able to access their email via WorldClient and whether or not users will be able to configure their accounts via WebAdmin. In addition, if you are granting access to WebAdmin, you can control which settings that accounts will be allowed to edit.



Web-based mail access defaults

☑ Account can access email via WorldClient

If selected accounts will be able to access mail via the web by default.

Web-based remote configuration defaults

☑ Account can modify its own settings via WebAdmin

By default, accounts can do the following via WebAdmin:

☐ Edit Real name
☑ Edit Password
☐ Edit mail directory location
☑ Edit forwarding address
☐ Edit advanced forwarding
☐ Edit encrypt mail setting
☑ Edit IMAP rules (PRO version only)
☐ Edit EVERYONE list setting
☐ Edit mail restrictions
☐ Edit quota settings
☐ Edit MultiPOP settings
☑ Edit autoresponder settings
☐ Edit allow changes via email

Accounts will have these default WebAdmin rights.

Web-based Mail Access Defaults

Account can access email via WorldClient
Enable this checkbox if you would like new accounts to be able to access the WorldClient server, which enables them to check their email via a web browser.

Web-based Remote Configuration Defaults

Account can modify its own settings via WebAdmin
Enable this feature if you want to grant MDaemon users permission to modify their account settings via WebAdmin. They will only be able to edit those settings that you designate on this dialog.

When this feature is enabled, and the WebAdmin server is set to *Active* on the Message Router, users will be able to log in to WebAdmin using their browser by pointing it to **http://mdaemonsdomain.com:Port**. They will first be presented with a logon screen and then a screen that contains the settings that they have been given permission to edit. All they need to do is edit whatever settings they choose and then click the *Save Changes* button. They can then close their browser; there is no need to logoff or do anything further.

Accounts that have been given administrative permission (designated on the individual account's Web tab) will see a different screen after they log in to WebAdmin. For a discussion on the administrative options within WebAdmin, see the WebAdmin user manual.

By default, accounts can do the following via WebAdmin:

Edit real name
Enabling this feature will allow users to modify their *Real Name* setting.

Edit password
Click this checkbox if you wish to allow users to modify their *POP Password.*

Edit mail directory location
This control is used to give users permission to modify the location of their *Message Directory*.

Note

You should exercise caution in granting this permission to users. Giving users the ability to change their mail directory could effectively give them access to any directory on your system.

Edit forwarding address
When this feature is enabled users will be able to modify their forwarding address settings.

Edit advanced forwarding
When this feature is enabled users will be able to modify their *Advanced Forwarding Options*.

Edit encrypt mail setting
This feature allows users to control whether or not mail messages of 4096 bytes or less will be stored in their mailbox in an encrypted state.

Edit IMAP rules (PRO version only)
Use this control to enable users to create and manage their own IMAP Mail Rules (see page 240). This feature is only available in MDaemon PRO.

Edit EVERYONE list setting
This feature allows users to control whether or not they will be included on MDaemon's `EVERYONE` *Mailing List*.

Edit mail restrictions
This checkbox controls whether or not accounts will be able to edit their "local mail only" settings.

Edit quota settings

Click this checkbox if you wish to allow accounts to modify their quota settings.

Edit MultiPOP settings

Click this switch if you wish users to be able to enable and disable MultiPOP collection.

Note

This permission doesn't grant users the ability to create, delete, or edit MultiPOP entries in any way. MultiPOP entries must be created by the administrator using the MDaemon interface. This feature is for allowing users to control whether or not MultiPOP Mail Collection for their account is turned on.

Edit autoresponder settings

Click this checkbox if you want users to be able to add, edit, or delete AutoResponders for their account.

Edit allow changes via email

Click this checkbox if you wish to allow users to modify their *Account Settings* via specially formatted email messages.

Apply these defaults to all accounts now

Click this button to cause these default settings to be applied to all MDaemon accounts. Any alternate settings that have been specified under individual accounts will be lost; the Web settings of all current MDaemon users will be changed to the settings specified here.

Chapter

20

Account Editor

Using MDaemon's Account Editor to create and edit accounts.

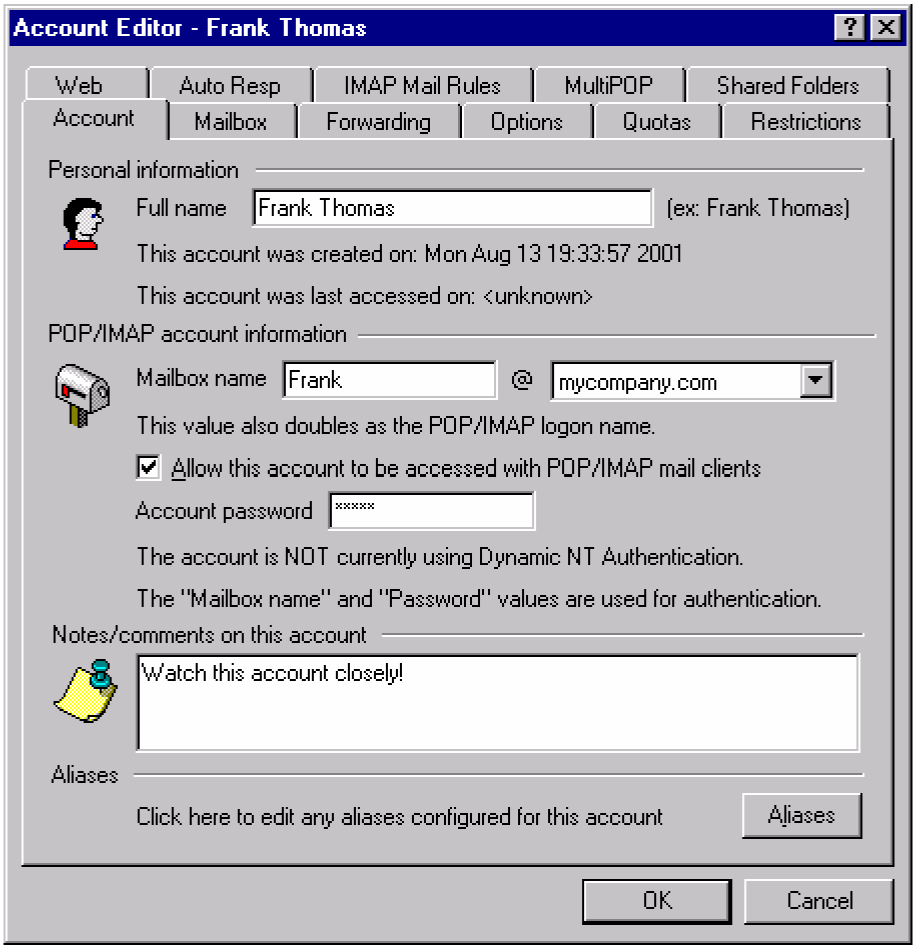
The Account Editor contains all settings specific to MDaemon accounts. It is used for creating new user accounts and for editing existing accounts. When creating a new account, most fields will be automatically filled in while typing the Real Name of the user. This auto-generated information is based on the templates and settings found in New Account Defaults (page 216).

See:

Account Manager—page 214
New Account Defaults—page 216
Creation an MDaemon User Account—page 215

Account Editor

Account



Personal information

Full name: Frank Thomas (ex: Frank Thomas)

This account was created on: Mon Aug 13 19:33:57 2001

This account was last accessed on: <unknown>

POP/IMAP account information

Mailbox name: Frank @ mycompany.com

This value also doubles as the POP/IMAP logon name.

☑ Allow this account to be accessed with POP/IMAP mail clients

Account password: *****

The account is NOT currently using Dynamic NT Authentication.

The "Mailbox name" and "Password" values are used for authentication.

Notes/comments on this account

Watch this account closely!

Aliases

Click here to edit any aliases configured for this account

Personal Information

Full name

Enter the user's first and last name here. When setting up a new mail account, the templates are reapplied each time the value in this field is changed. Real names cannot contain "!" or "|".

POP/IMAP Account Information

Mailbox name

This field specifies a unique name for the mailbox, and is also used as the account's POP/IMAP logon. In addition, the Mailbox must be unique and cannot contain spaces. After entering the name of the mailbox, click the drop-down list box and choose the domain to which this account's mailbox will apply. MDaemon's Primary Domain will appear in this control by default. Mailbox names cannot contain "!" or "|".

Allow this account to be accessed with POP/IMAP mail clients

This switch governs whether or not POP and IMAP access to the mailbox is allowed.

Account password

Enter an account password in this field. Below this field you will see a short statement that will tell you whether or not Dynamic NT Authentication is being used for this account (see page 251).

Note

You should always provide Account Password information even if you do not wish to allow POP/IMAP access to the mail account. If you wish to disallow access then use the *Allow This Account To Be Accessed…* switch rather than leaving the Account Password field blank. In addition to POP session verification, user and password values are used to allow remote account manipulation and remote file retrieval.

Notes/Comments on this Account

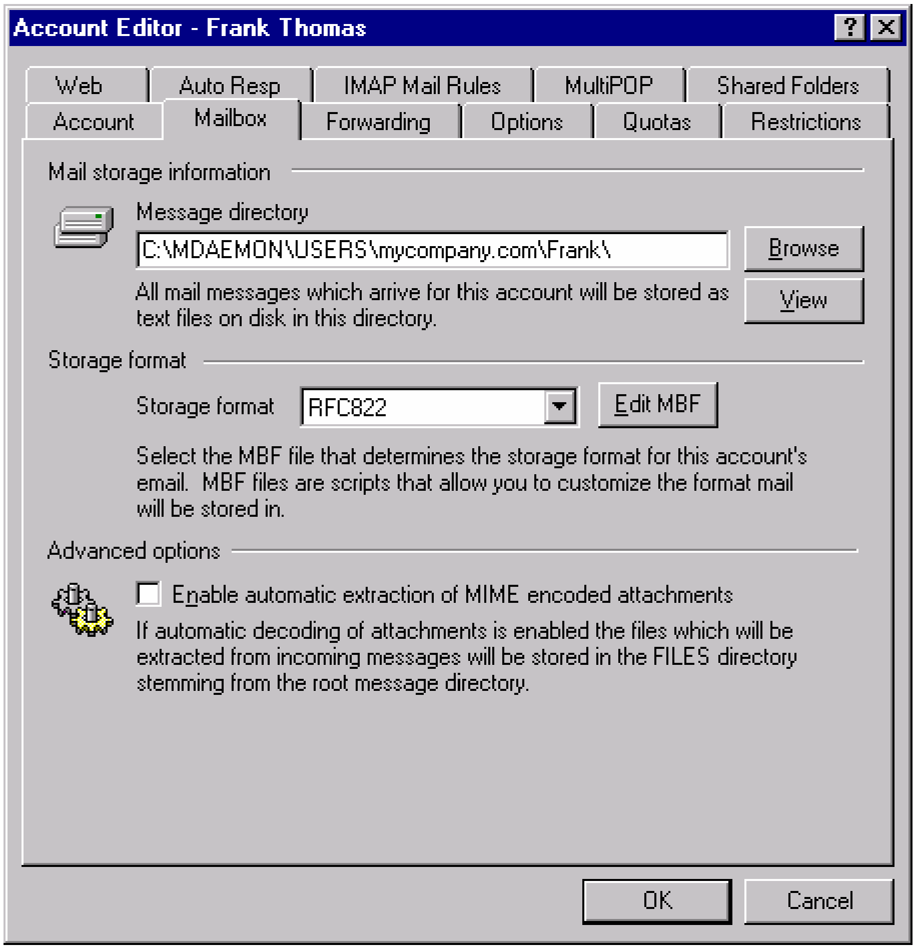
Use this text area for detailing any notes or comments regarding the account.

Aliases

Aliases

Click this button to open the Alias Editor, which will have the current account displayed and any aliases assigned to the account listed. You can use this dialog to edit previously configured aliases or create new ones.

Mailbox


Account Editor - Frank Thomas

Mail storage information

Message directory: C:\MDAEMON\USERS\mycompany.com\Frank\

All mail messages which arrive for this account will be stored as text files on disk in this directory.

Storage format

Storage format: RFC822

Select the MBF file that determines the storage format for this account's email. MBF files are scripts that allow you to customize the format mail will be stored in.

Advanced options

□ Enable automatic extraction of MIME encoded attachments

If automatic decoding of attachments is enabled the files which will be extracted from incoming messages will be stored in the FILES directory stemming from the root message directory.

Mail Storage Information

Message directory

Enter the directory where inbound mail messages destined for this account's mailbox should be placed.

Storage Format

Storage format

This window allows you to attach an MBF to the mailbox message directory. MBF files provide a method of mail system compatibility which may be useful in integrating your existing mail system with **MDaemon Server v6**. For a complete discussion of MBF files and how to construct them see **Creating and using MBF files** .

Edit MBF

This button will allow easy editing of the account's MBF file.

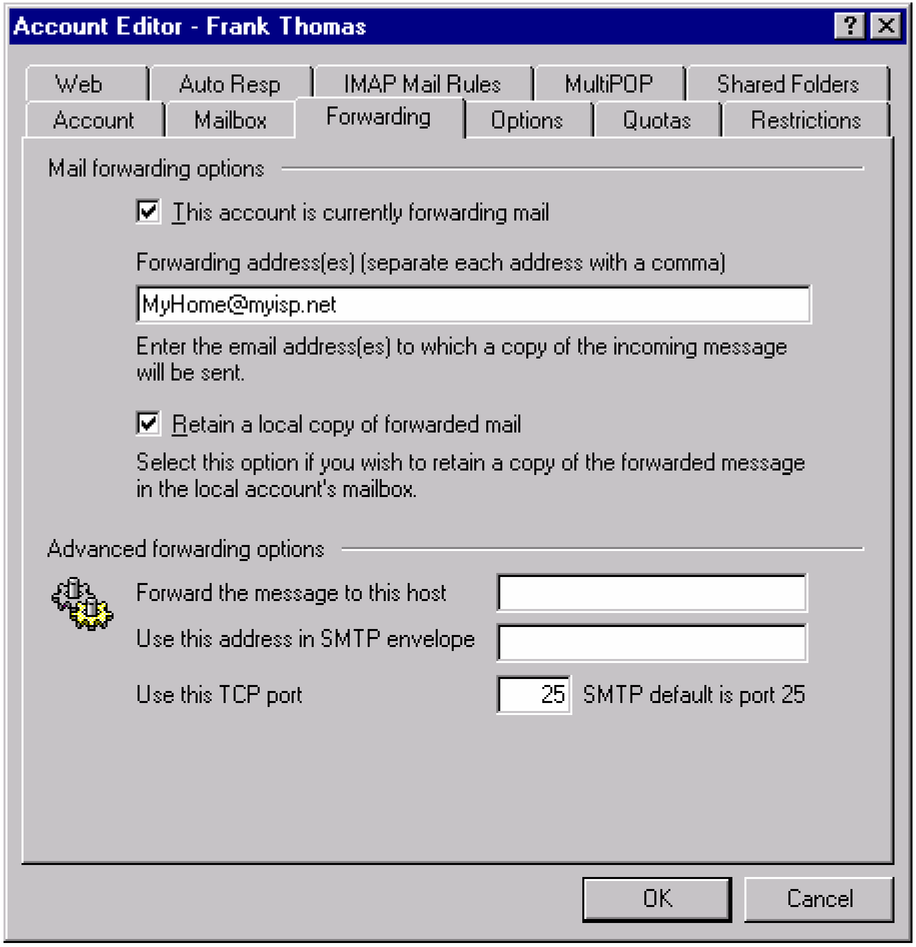
Advanced Options

Enable automatic extraction of MIME encoded attachments

If set, this switch causes **MDaemon Server v6** to automatically extract any Base64 MIME embedded file attachments found within incoming mail messages. Extracted files are removed from the incoming mail message, decoded, and placed in the account's *File Directory*. A notice is placed within the textual portion of the mail message in place of the encoded data which states where the file was placed and what the file name is. This feature is extremely useful for mail transport systems and clients which do not have built in MIME capability or which require encoded parcels to be extracted and placed in separate directories from the textual portions of the mail message before being submitted into the mail stream.

User's who wish to access their accounts through POP agents such as Eudora or the Windows Exchange client may wish this option to be turned off (not set) as more powerful email client software can properly handle MIME Base64 encoded attachments.

Forwarding



Mail forwarding options

☑ This account is currently forwarding mail

Forwarding address(es) (separate each address with a comma)

MyHome@myisp.net

Enter the email address(es) to which a copy of the incoming message will be sent.

☑ Retain a local copy of forwarded mail

Select this option if you wish to retain a copy of the forwarded message in the local account's mailbox.

Advanced forwarding options

Forward the message to this host

Use this address in SMTP envelope

Use this TCP port 25 SMTP default is port 25

Mail Forwarding Options

<u>This account is currently forwarding mail</u>

This switch governs whether or not mail will be forwarded to the address specified in the *Forwarding Address* field.

<u>Forwarding address(es)</u>

This field allows you to specify an address where copies of all inbound mail messages destined for this account will be automatically forwarded once they arrive at the server and are delivered to the account's local mail directory. A copy of each new message arriving at the server will be automatically generated and forwarded to the address specified in this field provided the *This Account Is Currently Forwarding Mail* switch is selected.

<u>Retain a local copy of forwarded mail</u>

If the account is forwarding mail to another address it may not be necessary for MDaemon to retain a copy of the message in the users local mailbox. This switch governs that action.

Advanced Forwarding Options

Forward the message to this host

If a mail host is specified here the forwarded message will be delivered to it rather than to the domain specified by the value found in the *Forwarding Address* field.

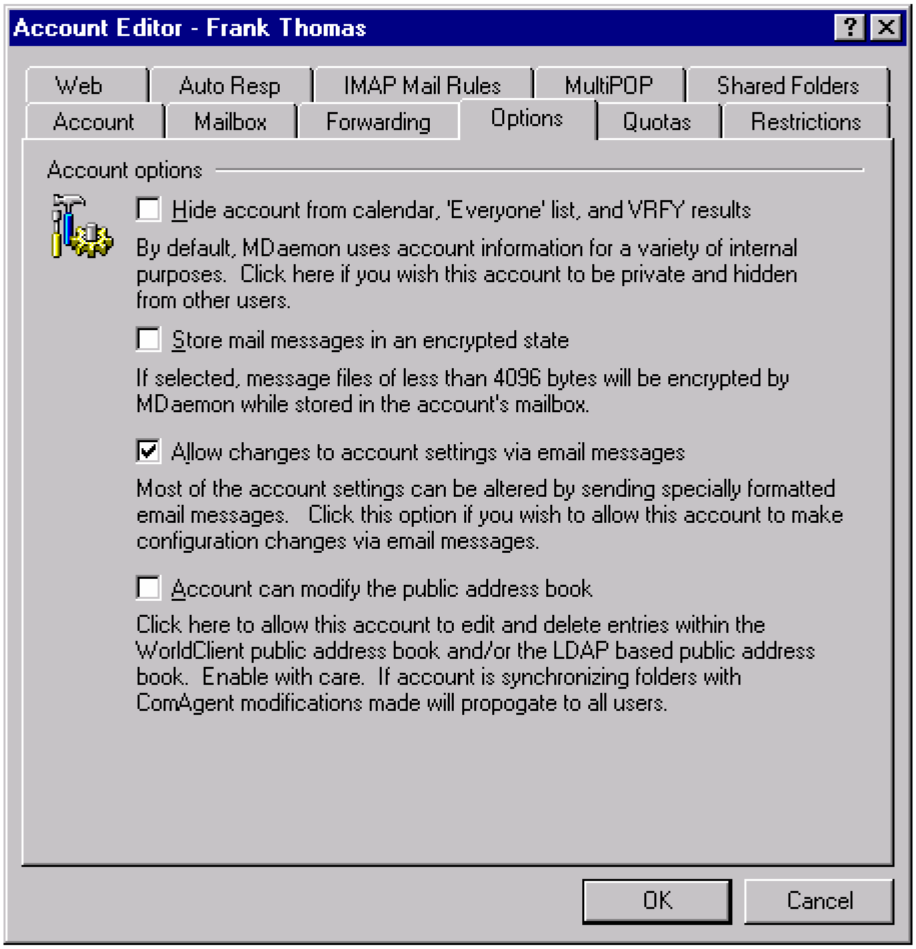
Use this address in SMTP envelope

If an address is specified here, this address will be used in the SMTP "Mail From:" statement used during the session handshaking with the accepting host. Normally, the sender of the message is used in this portion of the SMTP envelope. If you require an empty SMTP "Mail From:" command (looks like this: MAIL FROM <>) then enter "[trash]" into this control.

Use this TCP port

MDaemon will send this message on the TCP port specified here rather than the default SMTP outbound port.

Options



Account options

☐ Hide account from calendar, 'Everyone' list, and VRFY results

By default, MDaemon uses account information for a variety of internal purposes. Click here if you wish this account to be private and hidden from other users.

☐ Store mail messages in an encrypted state

If selected, message files of less than 4096 bytes will be encrypted by MDaemon while stored in the account's mailbox.

☑ Allow changes to account settings via email messages

Most of the account settings can be altered by sending specially formatted email messages. Click this option if you wish to allow this account to make configuration changes via email messages.

☐ Account can modify the public address book

Click here to allow this account to edit and delete entries within the WorldClient public address book and/or the LDAP based public address book. Enable with care. If account is synchronizing folders with ComAgent modifications made will propogate to all users.

Account Options

Hide account from the 'EVERYONE' list, LDAP address book, and VRFY results

MDaemon automatically creates and maintains a mailing list called **Everyone** which can be used to address each account on the server. By default MDaemon will include all accounts when it constructs the **Everyone** mailing list. Uncheck this switch if you want the account to be private and hidden from other users. This will also hide the account from the LDAP address book and VRFY results.

Store mail messages in an encrypted state

If selected, MDaemon will store mail for this account in an encrypted state. The messages will not be directly readable while in this state and should provide a very good level of protection. MDaemon will decrypt the message when it is transmitted via POP to the account holder but while stored on disk this account's message files will be encrypted.

Allow changes to account settings via email messages

This switch determines whether the user has access to account variables through remote email messages. This feature allows the user to perform common account maintenance such as changing passwords or mail directories by sending specially formatted mail messages to the server. For a complete discussion on remote account manipulation see **Remote Server Control Via Email** .

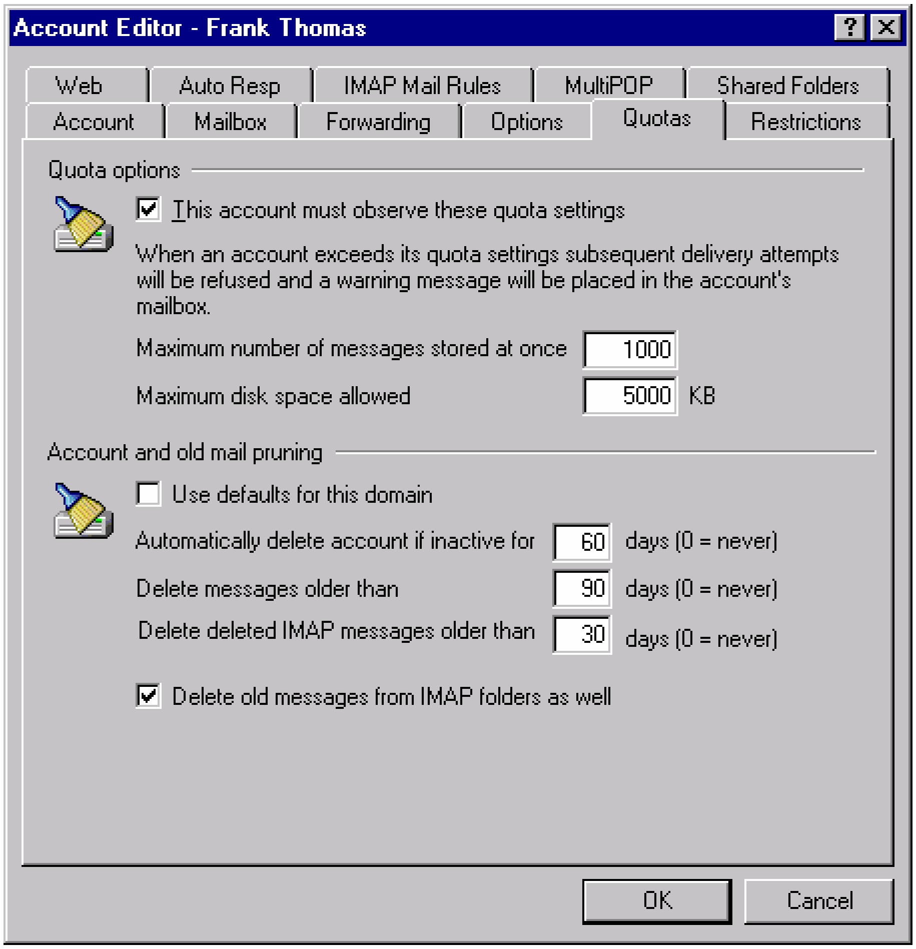
Account can modify the public address book

Click this option if you want the account to be able to add and delete entries from the WorldClient or LDAP-based public address books.

Caution!

If the Account is synchronizing folders with ComAgent then modifications could be propagated to all users. Exercise caution when enabling this feature.

Quotas



Account Editor - Frank Thomas

Quota options

☑ This account must observe these quota settings

When an account exceeds its quota settings subsequent delivery attempts will be refused and a warning message will be placed in the account's mailbox.

Maximum number of messages stored at once: 1000

Maximum disk space allowed: 5000 KB

Account and old mail pruning

☐ Use defaults for this domain

Automatically delete account if inactive for: 60 days (0 = never)

Delete messages older than: 90 days (0 = never)

Delete deleted IMAP messages older than: 30 days (0 = never)

☑ Delete old messages from IMAP folders as well

Quota Options

This account must observe these quota settings

Here you can specify the account's maximum number of allowable messages and the maximum amount of disk space (in kilobytes) that the account can consume (this includes any decoded file attachments in the account's *File Directory*). If a mail delivery to the account is attempted which would exceed the maximum messages limit or the maximum disk space allocated then the message is forwarded to the postmaster along with an appropriate warning. If a MultiPOP collection would exceed the account's maximum a similar warning is issued and the account's MultiPOP entries are automatically switched off (but not removed from the database).

Account and Old Mail Pruning

The controls in this section are used to designate when or if this account will be deleted by MDaemon if it becomes inactive. You can also designate whether or not old messages belonging to the account will be deleted after a certain time period. Each day at midnight, MDaemon will remove all messages that have exceeded the time limits stated, or it will delete the account completely if it has reached the inactivity limit. The default controls for these settings are located in the Primary Domain Configuration (page 53) and Secondary Domains (page 63) dialogs, but the controls on this tab can be used instead if you want this account's settings to override the domain defaults.

Use defaults for this domain

If you want to use the default Account and Old Mail Pruning settings for the domain to which this account belongs then click this checkbox. The default settings are located on either the Primary Domain Configuration (page 53) or Secondary Domains (page 63) dialog, depending on which type of domain the account belongs to.

Automatically delete account if inactive for XX days (0 = never)

Specify the number of days that you wish to allow the account to be inactive before it will be deleted. A value of "0" in this control means that the account will never be deleted due to inactivity.

Delete messages older than XX days (0 = never)

A value specified in this control is the number of days that any given message may reside in the account's mailbox before it will be deleted by MDaemon automatically. A value of "0" means that messages will never be deleted due to their age.

Delete deleted IMAP messages older than XX days (0 = never)

Use this control to specify the number days that you wish to allow IMAP messages that are flagged for deletion to remain in this user's folders. Messages flagged for deletion longer than this number of days will be purged. A value of "0" means that messages flagged for deletion will never be purged due to their age.

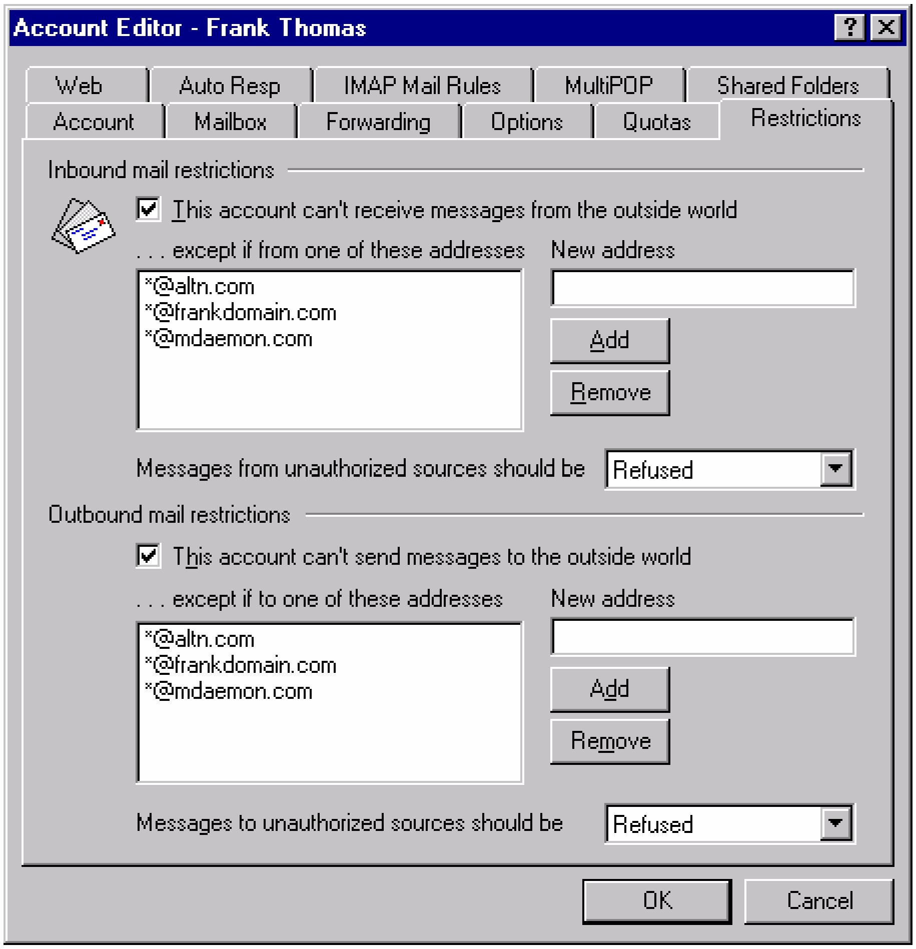
Delete old messages from IMAP folders as well

Click this checkbox if you want the "*Delete messages older than…*" control to apply to messages in IMAP folders as well. When this control is disabled, messages contained in IMAP folders will not be deleted, regardless of their age.

Note

When old messages are pruned, rather than actually delete them, MDaemon will move them to the "`...\BADMSGS\[Mailbox]\`" folder where they can be manually deleted later by the administrator or a nightly process. This only applies to pruned old messages – when an account is pruned, it will be deleted along with its messages instead of moved. See `AccountPrune.txt` in the "...`MDaemon\App\`" folder for more information and command line options.

Restrictions



Inbound mail restrictions

☑ This account can't receive messages from the outside world

. . . except if from one of these addresses

*@altn.com
*@frankdomain.com
*@mdaemon.com

New address

Messages from unauthorized sources should be: Refused

Outbound mail restrictions

☑ This account can't send messages to the outside world

. . . except if to one of these addresses

*@altn.com
*@frankdomain.com
*@mdaemon.com

New address

Messages to unauthorized sources should be: Refused

Use the controls on this tab to govern whether or not the displayed account will be able to send or receive mail to or from non-local domains (domains located somewhere other than your Local Area Network). There is a switch on the New Account Defaults dialog (page 216) for designating whether or not new accounts will have this restriction enabled by default.

Inbound Mail Restriction

This account can't receive messages from the outside world

Click this checkbox if you want the displayed account to be prevented from receiving email messages from non-local domains.

…except if from one of these addresses

Addresses specified in this area are exceptions to the Inbound Mail restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then all inbound messages from any address at altn.com would be accepted and delivered to the account.

New address

If you wish to add an address exception to the Inbound Mail Restrictions list then type it here and click the add button.

Add
After entering an address into the *New address* control, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

Messages from unauthorized sources should be…
The options in this drop-down list box govern what MDaemon will do with messages that are destined for this account but originate from a non-local or otherwise unauthorized domain. You may choose any of the following options:

Refused – Restricted messages will be refused by MDaemon.

Returned to sender – Messages from restricted addresses will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of this account.

Outbound Mail Restriction

This account can't receive messages to the outside world
Click this checkbox if you want the displayed account to be prevented from sending email messages to non-local domains.

…except if from one of these addresses
Addresses specified in this area are exceptions to the Outbound Mail restriction. Wildcards are permitted. Thus if you designated "*@altn.com" as an exception then all outbound messages to any address at altn.com would be delivered normally by MDaemon.

New address
If you wish to add an address exception to the Outbound Mail Restrictions list then type it here and click the add button.

Add
After entering an address into the *New address* control, click this button to add it to the exceptions list.

Remove
If you wish to remove an address from the restrictions list, select the address and then click this button.

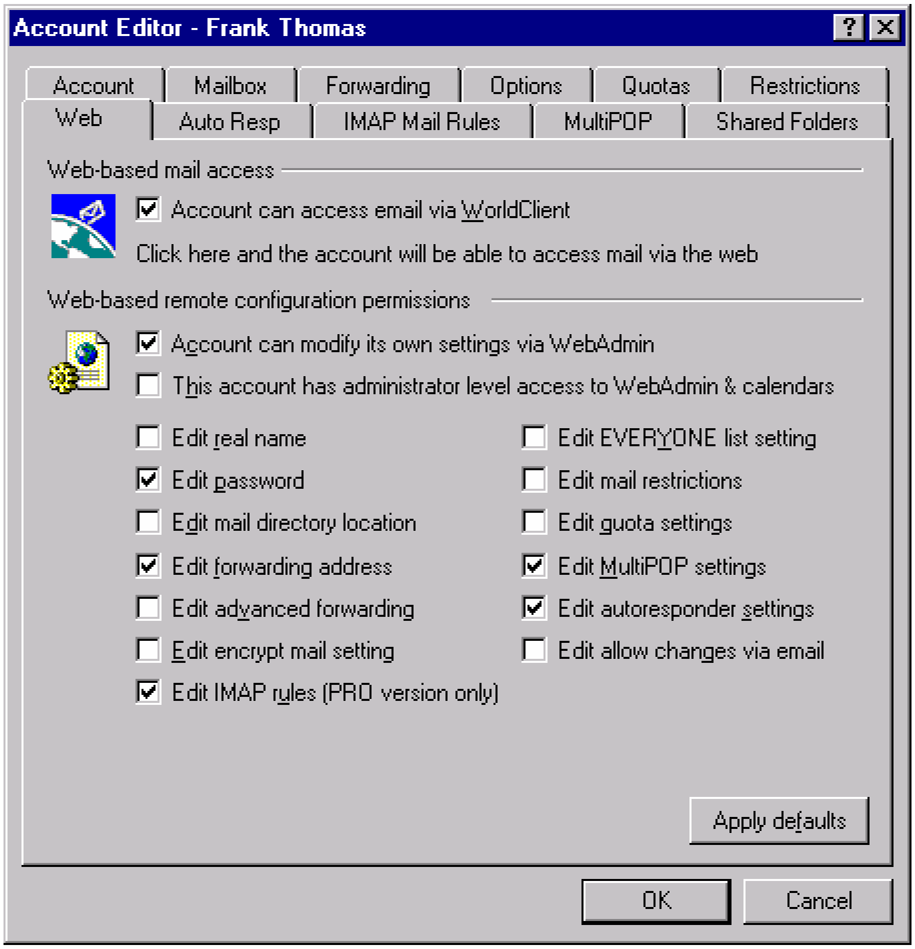
Messages to unauthorized sources should be…
The options in this drop-down list box govern what MDaemon will do with messages that originate from this account but are destined for a non-local or otherwise unauthorized domain. You may choose any of the following options:

Refused – Messages to unauthorized addresses will be refused by MDaemon.

Returned to sender – Messages from restricted addresses will be returned to the sender.

Sent to postmaster – Messages that are restricted will be accepted but delivered to the postmaster instead of the designated recipient.

Web



Web-based mail access

☑ Account can access email via WorldClient

Click here and the account will be able to access mail via the web

Web-based remote configuration permissions

☑ Account can modify its own settings via WebAdmin

☐ This account has administrator level access to WebAdmin & calendars

☐ Edit real name
☑ Edit password
☐ Edit mail directory location
☑ Edit forwarding address
☐ Edit advanced forwarding
☐ Edit encrypt mail setting
☑ Edit IMAP rules (PRO version only)
☐ Edit EVERYONE list setting
☐ Edit mail restrictions
☐ Edit quota settings
☑ Edit MultiPOP settings
☑ Edit autoresponder settings
☐ Edit allow changes via email

Web-based Mail Access

Account can access email via WorldClient

Enable this checkbox if you want the account to be able to access the WorldClient server, which enables them to check their email using a web browser.

Web-based Remote Configuration Permissions

Account can modify its own settings via the WebAdmin

Enable this feature if you wish to grant the MDaemon user permission to modify their account settings via WebAdmin. They will only be able to edit those settings that you enable below.

When this feature is enabled, and the WebAdmin server is set to *Active* on the Message Router, user will be able to log in to WebAdmin using their browser by pointing it to **http://mdaemonsdomain.com:Port**. They will first be presented with a logon screen and then a screen that contains the settings that they have been given permission to edit. All they need to do is edit whatever settings they choose and then click the *Save changes* button. They can then close their browser; there is no need to logoff or do anything further.

If the user has been given administrative permission (by enabling *This account can edit other users and mdaemon via the web*) they will see a different screen after they log in to WebAdmin. For a discussion on the administrative options within WebAdmin, see the WebAdmin section of this manual.

This account has administrator level access to WebAdmin

Enable this checkbox to grant the user administrative access to WebAdmin. This will give the user complete access to MDaemon's files and options via the web. For a discussion on the administrative options within WebAdmin, see the WebAdmin user manual.

Edit real name

Enabling this feature will allow the user to modify their *Real Name* setting.

Edit password

Click this checkbox if you wish to allow the user to modify their *Account Password.*

Edit mail directory location

This control is used to give the user permission to modify their *Message Directory* location.

Caution!

You should exercise caution in granting this permission to users. Giving users the ability to change their mail directory could effectively give them access to any directory on your system.

Edit forwarding address

When this feature is enabled, the user will be able to modify their forwarding address settings.

Edit advanced forwarding

When this feature is enabled, the user will be able to modify their *Advanced Forwarding Options.*

Edit encrypt mail setting

This feature allows the user to control whether or not mail messages of 4096 bytes or less will be stored in their mailbox in an encrypted state.

Edit IMAP rules (PRO version only)

Use this control to enable users to create and manage their own IMAP Mail Rules (see page 240). This feature is only available in MDaemon PRO.

Edit EVERYONE list setting

This feature allows the user to control whether or not they will be included on MDaemon's `EVERYONE` *Mailing List.*

Edit quota settings

Click this checkbox if you wish to allow the account to modify their quota settings.

Edit MultiPOP settings

Click this switch if you wish the user to be able to enable and disable MultiPOP collection.

This control doesn't grant the user the ability to create, delete, or edit MultiPOP entries in any way. MultiPOP entries must be created by the administrator using the MDaemon interface. This feature is for allowing users to control whether or not MultiPOP Mail Collection for their account is turned on.

Edit autoresponder settings

Click this checkbox if you want the user to be able to add, edit, or delete AutoResponders for their account.

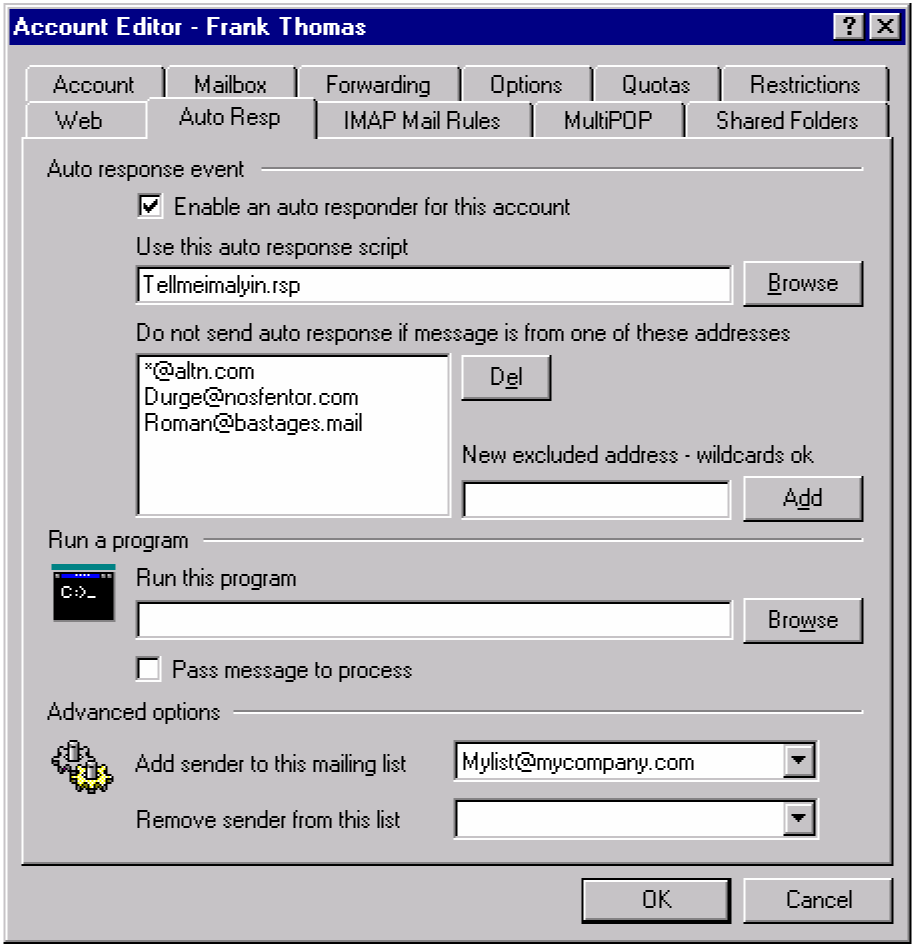
Edit allow changes via email

Click this checkbox if you wish to allow the user to modify their *Account Settings* via specially formatted email messages.

Apply defaults

Click this button to cause the default settings designated on the Web Access Defaults dialog (page 218) to be applied to this MDaemon account. Any alternate settings that have been specified on this individual's account will be replaced by the Web Access Defaults settings.

Auto Responder



☑ Enable an auto responder for this account

Use this auto response script: Tellmeimalyin.rsp

Do not send auto response if message is from one of these addresses:
*@altn.com
Durge@nosfentor.com
Roman@bastages.mail

New excluded address - wildcards ok:

Run this program:

□ Pass message to process

Add sender to this mailing list: Mylist@mycompany.com

Remove sender from this list:

Auto Response Event

Enable an auto responder for this account

Enable this control to activate an auto responder for the account. For more information on auto responders see:

Auto Responders and MBF Files—page 259

Use this auto response script

This field specifies the full path and filename of the response file (`*.RSP`) that will be processed and dispatched to the message sender. This file will first be passed through the filtering mechanism associated with MBF files. Any template string available for use in an MBF file will also be available for use in an auto-response file.

See:

Creating Auto Response Scripts—page 261
Creating and Using MBF Files—page 263

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this Auto Responder.

Note

Occasionally Auto Response messages may be sent to an address that returns an Auto Response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. You can use this feature to prevent an MDaemon Auto Responder from sending responses to one or more of these addresses by entering them here.

Del
Click this button to delete selected entries from the list of excluded addresses.

New excluded address—wildcards okay
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Add
After entering an address in the *New Excluded Address* text box, click this button to add it to the list of excluded address.

Run a Program

Run this program
This field specifies the full path and filename to a program that will be launched when new mail arrives at the specified mailbox. Care must be taken to ensure that this process terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run This Process* field will be passed the name of the triggering message as the first available command line parameter. Note that by the time the message name is passed to the specified process the account's MBF file will already have been applied. This is useful in that applying an MBF can reformat the message into a consistent structure regardless of the source of the original message. When the auto responder is setup on an account which is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see **Forwarding**—page 226) then this function will be disabled.

Note

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible: `logmail /e /j /message=$MESSAGE$ /q`

Advanced Options

Add sender to this mailing list

If a mailing list is entered in this field then the sender of the mail message will be automatically joined to that mailing list. This is a very handy feature for building automatic lists.

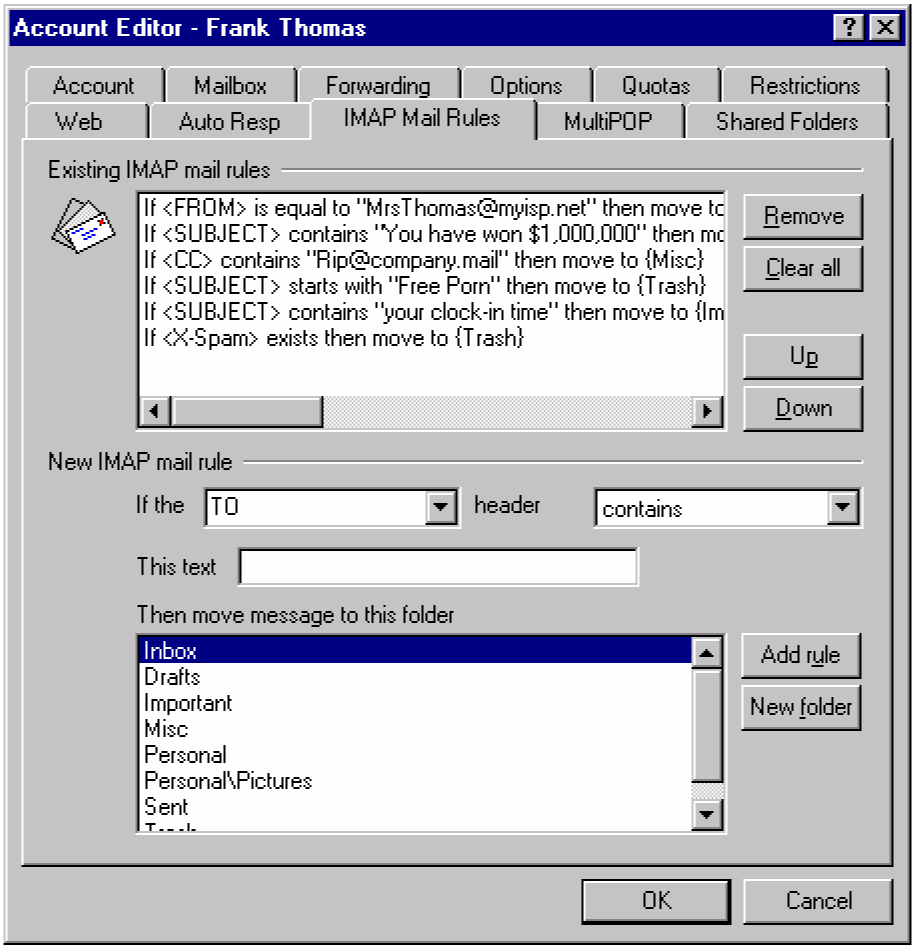
Remove sender from this mailing list

If a mailing list is entered in this field then the sender of the mail message will be automatically removed from the specified mailing list.

Tip

Auto-Response events are always honored when the triggering message is from a remote source. For messages originating locally, whether or not an Auto Responder will but triggered is contingent upon a setting on the **Miscellaneous Options** dialog (page 194). The control is: *Auto Responders are triggered by Local as well as Remote Traffic.* Enable the control if you want Local mail to trigger an auto response.

IMAP Mail Rules



```
If <FROM> is equal to "MrsThomas@myisp.net" then move tc
If <SUBJECT> contains "You have won $1,000,000" then mc
If <CC> contains "Rip@company.mail" then move to {Misc}
If <SUBJECT> starts with "Free Porn" then move to {Trash}
If <SUBJECT> contains "your clock-in time" then move to {Im
If <X-Spam> exists then move to {Trash}
```

If the: TO header: contains

Then move message to this folder:

- Inbox
- Drafts
- Important
- Misc
- Personal
- Personal\Pictures
- Sent

With MDaemon, IMAP users can have their mail routed automatically to specific folders on the server. Similar to the Content Filters, MDaemon will examine the headers of each message and then compare them to rules. When a message for the account holder matches one of their rules, MDaemon will move it to the folder specified in that rule. This method is much more efficient (for both the client and server) than attempting to filter the messages at the client, and since some IMAP clients do not even support message rules or filtering, IMAP Mail Rules provides this functionality to them.

IMAP Mail rules and messages folders can be created directly on the server via the IMAP Mail Rules tab of the Account Editor. They can also be created by the users themselves via specially formatted email messages (see page 318). Support for managing IMAP Mail Rules has also been added to WebAdmin. By simply logging in to WebAdmin with their browser they can manage their own account rules and settings that you have given them permission to manage. Thus, by using WebAdmin you can give your users total control over their own rules and avoid having to manage those functions for them.

Existing IMAP Mail Rules

This box displays the list of all rules that have been created for the user's account. Rules are processed in the order in which they are listed until a match is found. Therefore, as soon as a message matches one of the rules it will be moved to the folder specified in that rule and then rule processing for that message will cease. Use the Up and Down buttons to move rules to different positions in the list.

Remove

Click a rule in the list and then click *Remove* to delete it from the list.

Clear all

Clicking this button will delete all of the user’s IMAP Mail Rules.

Up

Click a rule in the list and then click this button to move it to a higher position in the list.

Down

Click a rule in the list and then click this button to move it to a lower position in the list.

New IMAP Mail Rule

Use the controls in this section to create new IMAP Mail Rules for the users.

If the [message header] header

Type a message header into this box or choose one from the drop-down list. MDaemon will search this header in all of the account’s incoming messages for the text contained in the “*This text*” control below. Then, based upon the type of comparison being made, it will determine which messages should be moved to the rule’s specified folder.

Comparison drop-down list box

This is the type of comparison that will be made when a message’s headers are compared to the IMAP Mail Rule. MDaemon will search the specified header for the text contained in the “*This text*” field and then proceed based upon this control’s setting—does the header’s complete text match exactly, not match exactly, contain the text, not contain it at all, start with it, and so on.

This text

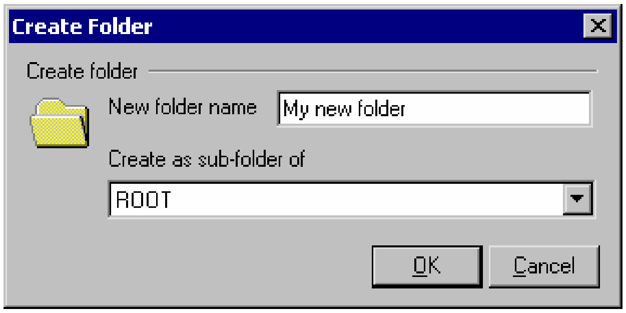
Enter the text that you want MDaemon to search for when scanning the message header that you have specified for the rule.

Then move message to this folder

After specifying the various parameters for the rule, click the folder that you want messages matching it to be moved to and then click the *Add rule* button to create it.

New folder

Click this button to create a new folder. This will open the Create Folder dialog on which you will assign a name for the folder. If you want it to be a subfolder of an existing folder then choose the folder from the drop-down list.



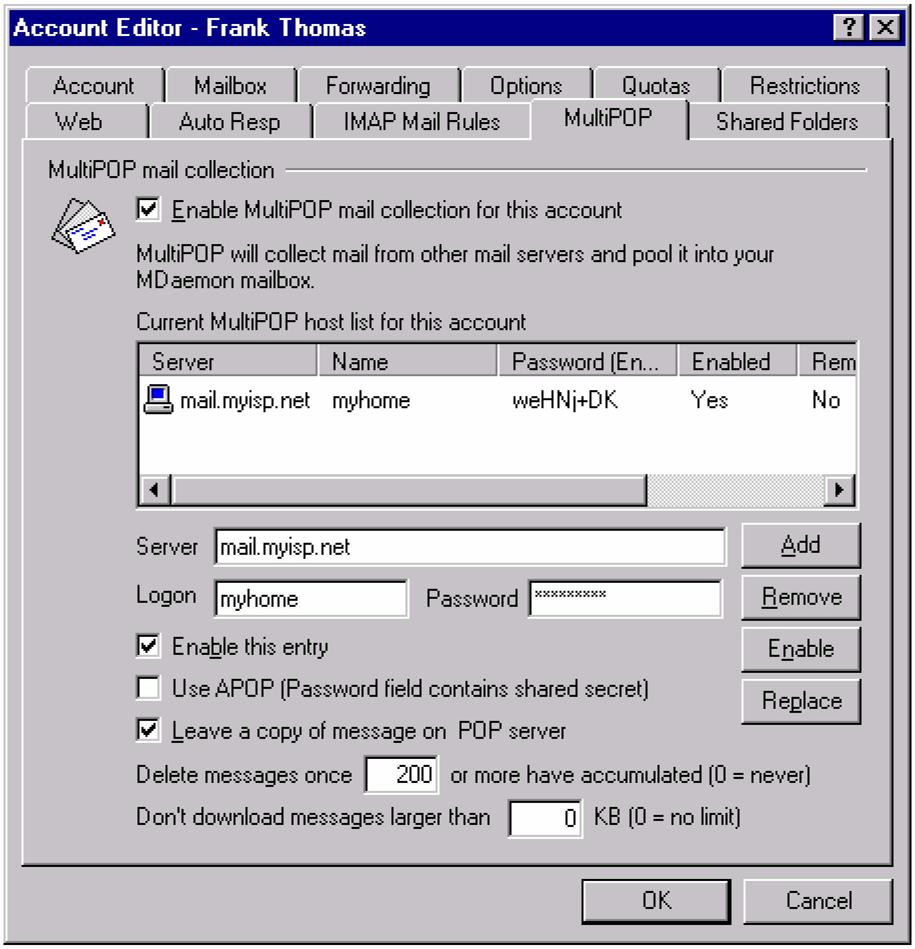
Create Folder

Create folder

New folder name: My new folder

Create as sub-folder of: ROOT

MultiPOP



MultiPOP mail collection

☑ Enable MultiPOP mail collection for this account

MultiPOP will collect mail from other mail servers and pool it into your MDaemon mailbox.

Current MultiPOP host list for this account

Server	Name	Password (En...	Enabled	Rem
mail.myisp.net	myhome	weHNj+DK	Yes	No

Server: mail.myisp.net

Logon: myhome Password: *********

☑ Enable this entry

☐ Use APOP (Password field contains shared secret)

☑ Leave a copy of message on POP server

Delete messages once 200 or more have accumulated (0 = never)

Don't download messages larger than 0 KB (0 = no limit)

The MultiPOP feature (located on the Account Editor) allows you to script an unlimited number of POP host/user/password combinations for collection of mail messages from multiple sources. This is useful for your users who have mail accounts on multiple servers but would prefer to collect and pool all their email together in one place. Before being placed in the user's mailbox, MultiPOP collected mail is first placed in the local queue so that it can be processed like other mail having autoresponders and Content filters applied to it.

Note

This editor uses advanced common controls that were not present in the original shipping versions of Windows 95. If the MultiPOP editor will not retain your settings then you need to download and install the newer common controls DLL file from Microsoft (www.microsoft.com).

MultiPOP Mail Collection

Enable MultiPOP mail collection for this account

This switch must be enabled for MultiPOP processing to occur for the account.

Server

Enter the POP3 server from which you wish to collect mail. Additionally, if you wish to specify a port to collect the mail from other than MDaemon's current default POP port, you can do so by appending a new port value to the host name separated by a colon. For example, using "`mail.altn.com`" as a MultiPOP host will connect to that host using the default outbound POP port while using "`mail.altn.com:523`" will connect to that host on port 523.

Logon

Enter the POP3 `USER` or `LOGON` name that accesses the mail account on the specified server.

Password

Enter the POP3 password or APOP shared secret used for accessing the mail account on the specified server.

Use APOP (password field contains shared secret)

Click this checkbox is you want the MultiPOP entry to use the APOP method of authentication when retrieving mail from its corresponding host. Note: The *Password* control must contain the APOP shared secret when this feature is chosen.

Leave a copy of message on POP server

Click this checkbox if you want to leave a copy of collected messages on the server. This is useful when you plan to retrieve these messages again at a later time from a different location.

Delete messages once [xx] or more have accumulated (0 = never)

This is the number of messages that MultiPOP will leave on the POP server before they will be deleted. When this number has accumulated, all stored messages will be deleted. Enter "0" into this control if you do not wish to place a limit on the number of messages that may be stored.

Note

Some ISP's limit the number of messages that may be stored so you should check with them about any restrictions that may apply to your account.

Don't download messages larger than [XX] KB (0 = no limit)

Enter a value here if you wish to limit the size of messages that may be downloaded.

Remove

Click this button to remove the selected MultiPOP entries from the list.

Enable/disable

Clicking this button toggles the state of the selected MultiPOP entries. This switch gives you control over whether MDaemon will collect mail for this entry or skip over it when it performs its MultiPOP processing.

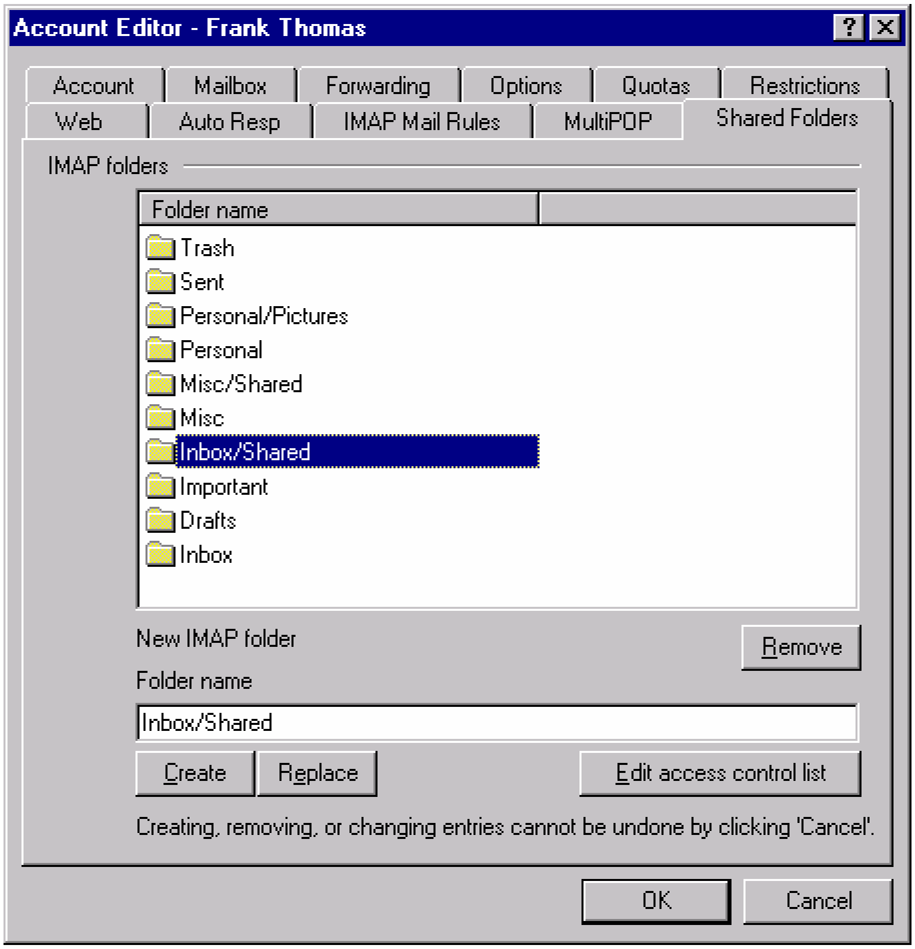
Add

Press this button to add your values to the list of MultiPOP records.

Replace

When an entry is selected from the list it will be presented for editing. After making any desired changes, click this button to apply them.

Shared Folders



Trash
Sent
Personal/Pictures
Personal
Misc/Shared
Misc
Inbox/Shared
Important
Drafts
Inbox

Folder name: Inbox/Shared

Creating, removing, or changing entries cannot be undone by clicking 'Cancel'.

IMAP Folders

This area displays all of the user's IMAP Folders and can be used to share access to them with other MDaemon users. When the account is first created, this area will be empty until you use the *Folder name* and *Create* controls (or the controls on the IMAP Mail Rules tab) to add a folder to it. Subfolders in this list will have the folder and subfolder names separated by the delimiter character designated on the Shared Folders tab of the Shared IMAP Folders dialog (click Setup→Shared IMAP Folders…→Shared Folders).

Remove
To remove a Shared IMAP folder from the list, select the desired folder and then click the Remove button.

New IMAP Folder

Folder name
To add a new folder to the list, specify a name for it in this control and click *Create*. If you want the new folder to be a subfolder of one of the folders in the list, then prefix the new folder's name with the parent folder's name and the delimiter character designated on the Shared Folders tab of the Shared IMAP Folders dialog. For example, if the delimiter character is '/' and the parent folder is "My Folder" then the

new subfolder name would be "My Folder/My New Folder". If you don't want it to be a subfolder then name the new folder "My New Folder" without the prefix.

Create

After specifying a folder's name click this button to add the folder to the list.

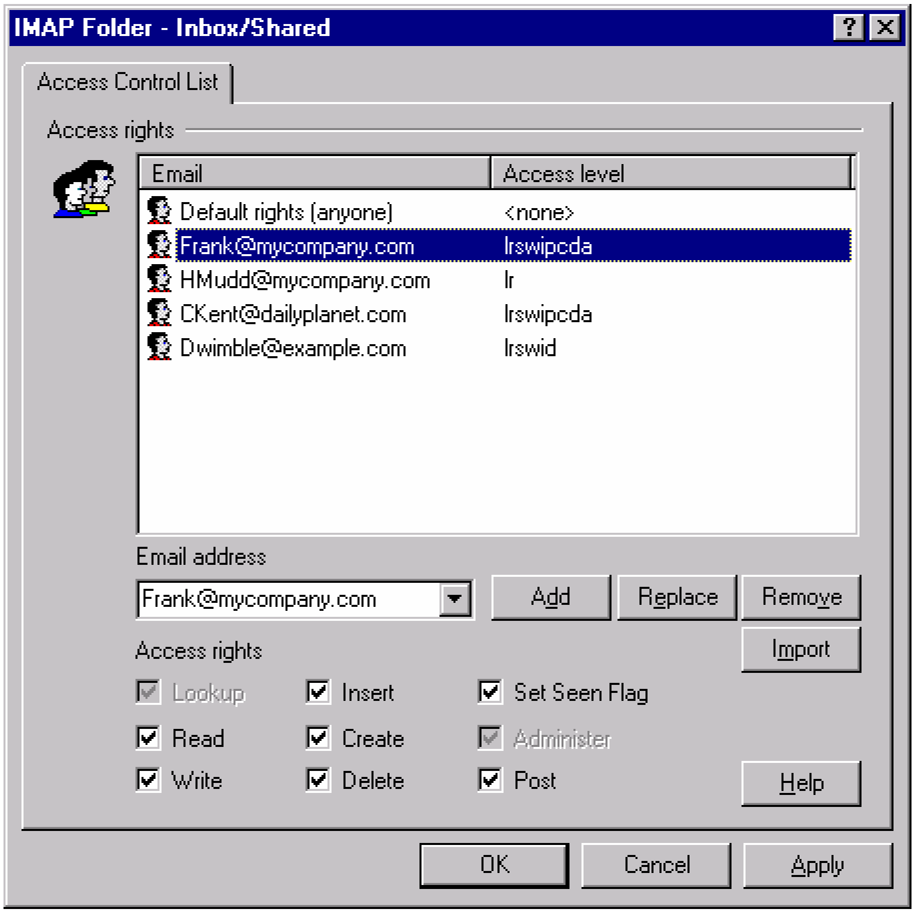
Replace

If you wish to edit one of the Shared Folders, click the entry, make the desired change, and then click *Replace.*

Edit access control list

Choose a folder and then click this button to open the Access Control List dialog for that folder. Use the Access Control List dialog to designate the users that will be able to access the folder and the permissions for each user.

Access Control List



Email	Access level
Default rights (anyone)	<none>
Frank@mycompany.com	lrswipcda
HMudd@mycompany.com	lr
CKent@dailyplanet.com	lrswipcda
Dwimble@example.com	lrswid

Email address: Frank@mycompany.com

Access rights

☑ Lookup	☑ Insert	☑ Set Seen Flag
☑ Read	☑ Create	☑ Administer
☑ Write	☑ Delete	☑ Post

Access Rights

This area is for designating the MDaemon user accounts that you wish to grant access to the shared folder, and for setting the access permissions for each one. You can reach this dialog from the Shared Folders tab of the Account Editor (click Accounts→Account Manager…→User Account→Shared Folders). Double-click the desired folder, or click the folder and then click *Edit access control list*, to open the Access Control dialog for that folder. Each entry lists the email address of the account and a one letter Access Level abbreviation for each Access Right that you grant to the user.

Email address
From the drop-down list, choose the MDaemon account that you wish to grant access to the shared folder.

Add
After choosing an Email Address from the list, and the access rights that you wish to grant to the user, click *Add* to add the account to the list.

Replace
To modify an existing Access Rights entry, select the entry, make any desired changes to the Access Rights, and then click *Replace*.

Remove

To remove an entry from the Access Rights list, select the desired entry and then click *Remove*.

Import

With the *Import* feature you can add the members of an existing Mailing List to the list of users with Access Rights. Choose the access rights that you wish to grant to the users, click Import, and then double-click the desired list. All of the list's members will be added to the list with the rights that you set.

Access Rights

Choose the rights that you wish to grant to individual users by clicking the desired options in this area and then clicking *Add* for new entries or *Replace* for existing entries.

You can grant the following Access Control Rights:

Lookup (l) – user can see this folder in their personal list of IMAP folders.

Read (r) – user can open this folder and view its contents.

Write (w) – user can change flags on messages in this folder.

Insert (i) – user can append and copy messages into this folder.

Create (c) – user can create subfolders within this folder.

Delete (d) – user can delete messages from this folder.

Set Seen Flag (s) – user can change the read/unread status of messages in this folder.

Administer (a) – user can administer the ACL for this folder.

Post (p) – user can send mail directly to this folder (if folder allows).

Help

Click *Help* to display a list of the access rights and their definitions.

Chapter

21

Importing Accounts

Importing user accounts into MDaemon.

MDaemon Server v6 supports multiple methods of importing user accounts. They may be imported from an NT SAM database, an SLMail user database, or directly from a text file. MDaemon's import features are reached from the **Accounts→Import** menu selection.

Importing Accounts From a Text File

Click the **Accounts→Importing…→Import accounts from a comma delimited text file…** menu selection to access this account generation feature. It can also be reached by clicking the *Import* button on the Account Manager (page 214). This is a simple method for importing and automatically generating mail accounts. MDaemon will read a text file and generate new mail accounts using as little as just the first and last names of the user. If you are careful to setup your account template strings properly (see **New Account Defaults**—page 216) you can generate unique accounts using only the first and last names, but you can also include many other options for specific user settings if you want to override the new account defaults. All fields must be separated by commas.

Each line of the comma delimited text file must contain only a single entry. The first line must be a base line giving the names and sequence of the fields in subsequent lines. A sample file would look something like this:

```
"Mailbox", "FullName", "MailDir", “AllowAccess”
"arvel", "Arvel Hathcock", "C:\Mail\Arvel\", Y
"frank", "Frank Thomas", "C:\Mail\Frank\", N
```

Note

The field names in the base line are used by MDaemon to determine the data sequence and can therefore appear in any order. Each of the field names must be in quotes.

All "String" values must be contained in quotes, and a "bool" field value is considered `FALSE` unless the first char is: `y`, `Y`, `1`, `t`, or `T`.

First, middle, and last names are acceptable in each full name. However, you may not use commas in them.

After running the import process, MDaemon will create `TXIMPORT.LOG`, detailing the import results and listing which accounts imported successfully and which failed. Typical reasons why an account might not be imported would include a conflict with an existing account's mailbox, name, or directory information, a conflict with an existing alias to an account, or a conflict with a mailing list name.

See the description of the `MD_ImportUserInfo()` and the `MD_ExportAllUsers()` within the `MD-API.HTML` file located in your `\API\` directory, for more information on the field mappings.

Use the following values in the base line to map to MDaemon account fields:

Field Name	Type
MailBox	string
Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	bool
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	int
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	bool
RemoveFromList	bool
PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int

MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	string

Windows NT Security Account Integration

MDaemon supports *Windows NT* integration. This support consists of a *Windows NT* user database import engine, which can be reached through the MDaemon menu selection **Accounts|Import|From NT SAM Database…**. Additionally, support for dynamic authentication of users has been embedded into the MDaemon user management code. It is possible to specify an NT domain in an account's password field and then MDaemon will dynamically authenticate such accounts in real-time, using the specified NT domain's security system. Under such a scheme, changing the account's password in the *Windows NT User Manager* will have the effect of automatically updating MDaemon. Therefore, your users will only have to remember one set of authentication credentials. This also makes for very easy account setup for new installations.

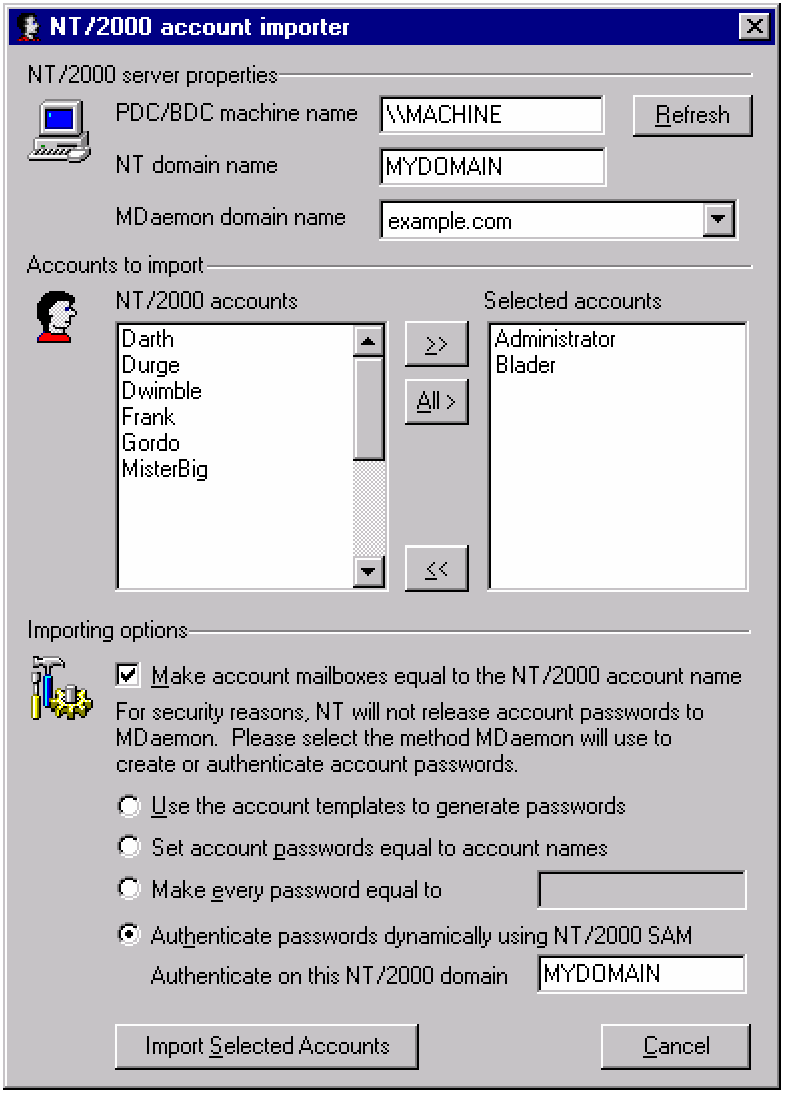
Important!

The security context of the account running MDaemon **must** have the **SE_TCB_NAME** privilege. If the process is a service running in the *Local System* account, it will have this privilege by default. Otherwise, it must be set by the following procedure:

Run the "*User Manager*" (NT Administration tool) and select "*User Rights*" from the "*Policies*" menu. **NOTE:** You must select the "*Show Advanced User Rights*" check box to see the **SE_TCB_NAME** privilege. The correct privilege, **SE_TCB_NAME**, is labeled "*To Act as Part of the Operating System*". Select this and "**Add**" this right to the account under which MDaemon operates. If you add this right you may need to restart MDaemon before it takes affect.

See Microsoft articles Q101366 and Q131144 for more detailed information.

NT To MDaemon Account Importer



NT/2000 server properties

PDC/BDC machine name: \\MACHINE

NT domain name: MYDOMAIN

MDaemon domain name: example.com

Accounts to import

NT/2000 accounts	Selected accounts
Darth	Administrator
Durge	Blader
Dwimble	
Frank	
Gordo	
MisterBig	

Importing options

☑ Make account mailboxes equal to the NT/2000 account name

For security reasons, NT will not release account passwords to MDaemon. Please select the method MDaemon will use to create or authenticate account passwords.

○ Use the account templates to generate passwords

○ Set account passwords equal to account names

○ Make every password equal to

● Authenticate passwords dynamically using NT/2000 SAM

Authenticate on this NT/2000 domain: MYDOMAIN

NT/2000 Server Properties

PDC/BDC Machine name

This field allows you to specify the machine name from which MDaemon will read NT account database information. You can specify \\<DEFAULT> and MDaemon will read data from the local machine.

Refresh

Click this button to refresh the NT Accounts listing.

NT Domain Name

Type the NT domain name from which you wish to import accounts.

MDaemon Domain Name

Choose from the drop-down list box the MDaemon domain into which the accounts will be imported.

Accounts to Import

NT/2000 accounts
This window contains a list of all the account names collected from the NT account database.

Selected accounts
This window contains all the account names that you have selected and wish to import.

>>
Click this button to move the highlighted account names from the "NT Accounts" window into the "Selected Accounts" window.

<<
Click this button to remove the highlighted entries from the "Selected Accounts" window.

Importing Options

Make account mailboxes equal to the NT/2000 account name
Click this switch to force each imported user's NT account name to be used as their Mailbox value. With this method, you will not need to worry about setting up the correct New Account Template macros (page 216).

Use the account template to generate passwords
This switch causes MDaemon to generate passwords for imported accounts using the account template settings (see New Account Defaults—page 216).

Set account passwords equal to account names
This switch causes MDaemon to use the account name as the account password.

Make every password equal to…
This switch allows you to specify a static password value that will be used by all imported accounts.

Authenticate passwords dynamically using NT/2000 SAM
This switch enables dynamic authentication of imported accounts. Rather than specifying a password MDaemon will simply authenticate the mail client supplied USER and PASS values using the NT database in real-time.

Authenticate on this NT/2000 domain
Enter the name of the Windows NT domain that MDaemon will use when authenticating connections dynamically. **This is not the machine name of the domain controller. It is the actual name of the NT Domain.**

Note

When accounts are configured for dynamic authentication on an NT machine the name of the NT domain preceded by two backslash characters is used in the account's `PASSWORD` field and is stored unencrypted within the `USERLIST.DAT` file. For example, if an account is configured for dynamic authentication on an NT domain called ALTN the account's password field will contain the value \\ALTN. The two backslash characters preceding the domain name trigger MDaemon that the password field actually contains the name of an NT domain and that MDaemon should attempt to authenticate the USER and PASS values provided by the mail client using that domain's account database. It is an error for a password to start with two backslash characters unless it is configured for dynamic authentication as described above. In other words, you can't just have regular passwords that start with two backslashes. Passwords beginning with two backslashes are always assumed to be providing an NT domain name and not a password. It is perfectly acceptable to enter two backslashes and the NT domain name into an account's password field using the regular Account Editor if necessary. The administrator need not restrict himself to using the importer in order to setup accounts for dynamic authentication.

Chapter

22

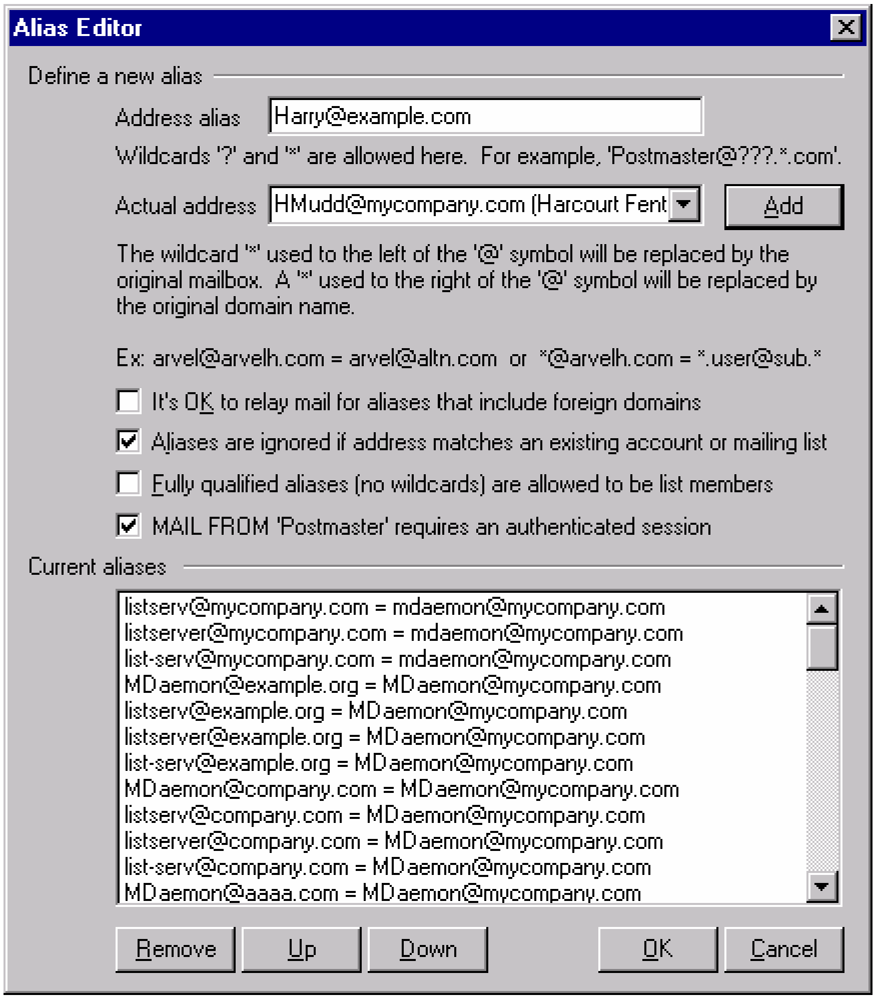
Address Aliases

Setting up Address Aliases.

The **Accounts|Address Aliases…** menu selection is used to open the Alias Editor. The Alias Editor makes it possible for you to create "fictitious" mailbox names for your accounts or mailing lists, which is extremely useful when you want multiple mailbox names resolved to a single user account or list. For example, if Frank@altn.com handled all billing inquiries to your domain, but you wanted to tell everyone to send them to Billing@altn.com, then you could create an Address Alias so that messages addressed to Billing@altn.com would actually go to Frank@altn.com. Or, if you were hosting multiple domains and wanted all messages addressed to the Postmaster (regardless of the domain) to go to a single user, then you could create the alias "Postmaster@*=Henry@altn.com".

Because a "Postmaster" must exist at each Internet mail site, MDaemon will check your defined aliases at program startup and issue a warning if you have failed to create such an alias.

Alias Editor



Define a new alias

Address alias: Harry@example.com

Wildcards '?' and '*' are allowed here. For example, 'Postmaster@???.*.com'.

Actual address: HMudd@mycompany.com (Harcourt Fent

The wildcard '*' used to the left of the '@' symbol will be replaced by the original mailbox. A '*' used to the right of the '@' symbol will be replaced by the original domain name.

Ex: arvel@arvelh.com = arvel@altn.com or *@arvelh.com = *.user@sub.*

☐ It's OK to relay mail for aliases that include foreign domains

☑ Aliases are ignored if address matches an existing account or mailing list

☐ Fully qualified aliases (no wildcards) are allowed to be list members

☑ MAIL FROM 'Postmaster' requires an authenticated session

Current aliases

```
listserv@mycompany.com = mdaemon@mycompany.com
listserver@mycompany.com = mdaemon@mycompany.com
list-serv@mycompany.com = mdaemon@mycompany.com
MDaemon@example.org = MDaemon@mycompany.com
listserv@example.org = MDaemon@mycompany.com
listserver@example.org = MDaemon@mycompany.com
list-serv@example.org = MDaemon@mycompany.com
MDaemon@company.com = MDaemon@mycompany.com
listserv@company.com = MDaemon@mycompany.com
listserver@company.com = MDaemon@mycompany.com
list-serv@company.com = MDaemon@mycompany.com
MDaemon@aaaa.com = MDaemon@mycompany.com
```

Define a New Alias

Address alias
Enter the email address for which you wish to create an alias. Wildcards of "?" and "*" are acceptable.

Actual address
Select an account from the drop-down list or type a new address or mailing list into this space. This is the actual address that will receive the message when it is addressed to a corresponding alias.

Add
Click the *Add* button to register the account alias request. The contents of the *Address Alias* and *Actual Address* fields will be combined and placed in the *Current Aliases* window.

It's OK to relay mail for aliases that include foreign domains
Click this control if you want MDaemon to relay mail for Address Aliases regardless of your Relay Control settings (page 125).

Aliases are ignored if address matches an existing account or mailing list

Sometimes you may want to create an alias that will be applied to some addresses but not others when they match an existing account. For example: you could create an alias using a wildcard stating that "*@mycompany.com=me@mycompany.com" which would cause all messages containing "@mycompany.com" to go to "me@mycompany.com" even if the addresses matched existing accounts. But, with this control activated only addresses that didn't match an account would have that alias applied to them.

Fully qualified aliases (no wildcards) are allowed to be list members

Click this checkbox if you want to allow address aliases to be members of MDaemon mailing lists. Only actual accounts can be list members if this control is not enabled. Note: address aliases containing wildcards are not permitted to be list members even if this control is enabled.

MAIL FROM 'Postmaster' requires an authenticated session

Click this checkbox to require the postmaster user's account to be authenticated before MDaemon will accept mail claiming to be from the 'Postmaster'. This will prevent unauthorized users from being able to present themselves as the domain's postmaster.

Current Aliases

This window contains all current Address Aliases that you have created.

Remove

Click this button to remove a selected entry from the *Current Aliases* list.

Up

Aliases are processed in the order in which they are listed. You can move an Alias to a higher position in the list by selecting it and then clicking this button.

Down

Aliases are processed in the order in which they are listed. You can move an Alias to a lower position in the list by selecting it and then clicking this button.

Chapter

23

Auto Responders and MBF Files

Creating and Using Auto Responders and MBF Files.

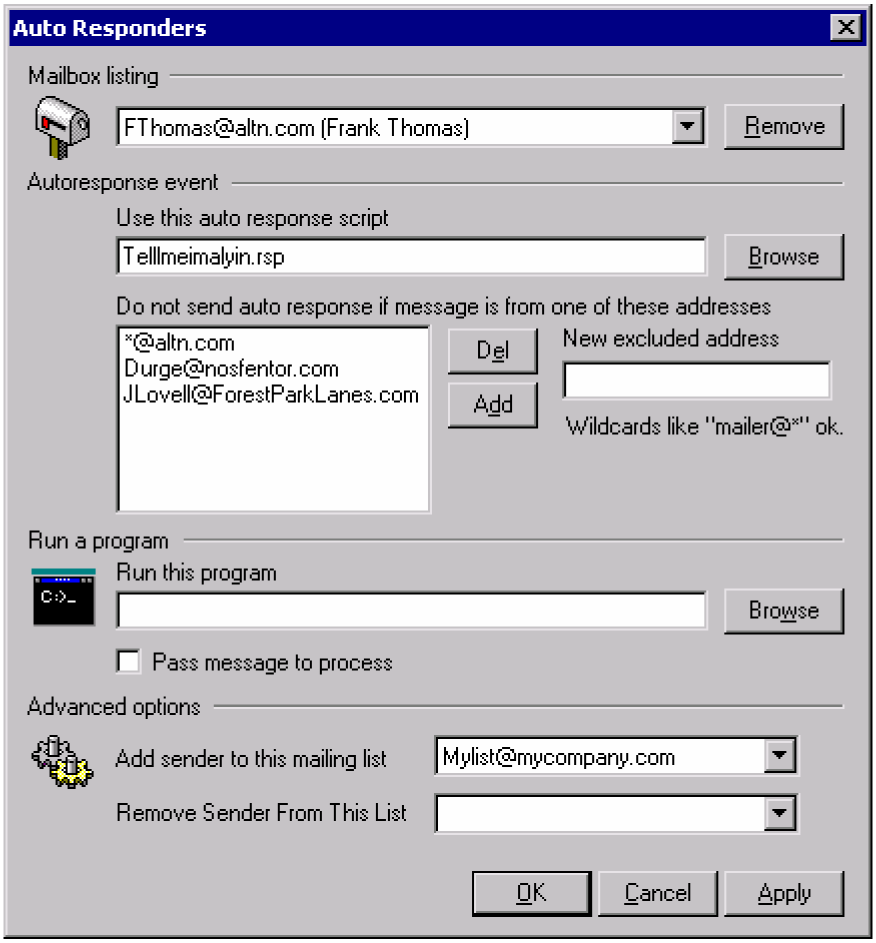
Auto responders are useful tools for automating events to be triggered by an incoming email message. One popular use for auto responders is to send back a user-defined message to any person who sends an email to a user who will be unable to read it due to a vacation, illness, or some other circumstance. Using the auto-response mechanisms provided with **MDaemon Server v6** (located in **Accounts|Auto Responders…**), incoming mail can act as a trigger generating automated and personalized replies or as the cause of a server hosted process in which the message itself is passed as a command line parameter. Automated response message files (`*.RSP` files) can contain any template string available to an MBF file (page 263).

MBF or Mailbox Format Files are text files designed to allow cross compatibility with other email transport systems that can accept ASCII text files into their mail streams. MBF files are essentially templates that contain a set of special formatting macros that enable MDaemon to transform an RFC-822 message into a variety of other text-based formats. Using MBFs, MDaemon can be configured to automatically reformat incoming mail into specific alternatives on a per mailbox basis. When a message arrives for an MDaemon account, the account's MBF file is used to reformat the incoming data before distributing it to the user.

See **Creating Auto Response Scripts**—page 261 for more information on creating automated response message files to be used by Auto Responders.

See **Creating and Using MBF Files**—page 263 for more information on MBF files.

Auto Responders



Auto Responders

Mailbox listing

FThomas@altn.com (Frank Thomas)

Autoresponse event

Use this auto response script

Telllmeimalyin.rsp

Do not send auto response if message is from one of these addresses

*@altn.com
Durge@nosfentor.com
JLovell@ForestParkLanes.com

New excluded address

Wildcards like "mailer@*" ok.

Run a program

Run this program

□ Pass message to process

Advanced options

Add sender to this mailing list: Mylist@mycompany.com

Remove Sender From This List:

Mailbox Listing

This control lists all available local mailboxes that can host an Auto Responder. Select a mailbox from this drop-down list and then fill in the desired auto response parameters to cause the Auto Responder to be triggered whenever a message arrives for the mailbox.

Remove
Clicking this button will remove any Auto Responder that is associated with the account selected in the *Mailbox* drop-down list box.

Autoresponse Event

Use this auto response script
This field specifies the full path and filename of the response file (`*.RSP`) that will be processed and dispatched to the message sender. This file will first be passed through the filtering mechanism associated with MBF files. Any template string available for use in an MBF file will also be available for use in an auto-response file.

See:

Creating Auto Response Scripts—page 261
Creating and Using MBF Files—page 263

Do not send auto response if message is from one of these addresses
Here you can list addresses that you wish to be excluded from responses initiated by this Auto Responder.

Note

Occasionally Auto Response messages may be sent to an address that returns an Auto Response of its own. This can create a "ping-pong" effect causing messages to be continually passed back and forth between the two servers. You can use this feature to prevent an MDaemon Auto Responder from sending responses to one or more of these addresses by entering them here.

Del
Click this button to delete selected entries from the list of excluded addresses.

Add
After entering an address in the *New Excluded Address* text box, click this button to add it to the list of excluded address.

New excluded address
If you wish to add an address to the list of excluded addresses enter it here and then click the *Add* button.

Run a Program

Run this program
This field specifies the full path and filename to a program that will be launched when new mail arrives at the specified mailbox. Care must be taken to ensure that this process terminates properly and can run unattended. Optional command line parameters can be entered immediately following the executable path if desired.

Pass message to process
Select this option and the process specified in the *Run This Process* field will be passed the name of the triggering message as the first available command line parameter. Note that by the time the message name is passed to the specified process the account's MBF file will already have been applied. This is useful in that applying an MBF can reformat the message into a consistent structure regardless of the source of the original message. When the auto responder is setup on an account which is forwarding mail to another location and **not** retaining a local copy in its own mailbox (see **Forwarding**—page 226) then this function will be disabled.

Note

By default, MDaemon will place the name of the message file as the last parameter on the command line. You can override this behavior by using the `$MESSAGE$` macro. Use this macro in place of where the message file name should be placed. This allows more flexibility in the use of this feature since a complex command line such as this will be possible: `logmail /e /j /message=$MESSAGE$ /q`

Add sender to this mailing list

If a mailing list is entered in this field then the sender of the mail message will be automatically joined to that mailing list. This is a very handy feature for building automatic lists.

Remove sender from this mailing list

If a mailing list is entered in this field then the sender of the mail message will be automatically removed from the specified mailing list.

Tip

Auto-Response events are always honored when the triggering message is from a remote source. For messages originating locally, whether or not an Auto Responder will but triggered is contingent upon a setting on the **Miscellaneous Options** dialog (page 194). The control is: *Auto Responders are triggered by Local as well as Remote Traffic.* Enable the control if you want Local mail to trigger an auto response.

Creating Auto Response Scripts

Auto Response scripts define the messages that are returned as the result of an auto-response event. They are constructed the same as MBF files and can contain the same macros (page 264). However, several additional macros are provided which allow you to develop more powerful auto-response messages.

In addition to those template variables defined for MBF files, auto-response scripts can use any or all of the following macros, which override the values parsed from the original message:

%SetSender%
ex: `%SetSender%=mailbox@host.org`
MDaemon will treat this address as if it had sent the original message.

%SetRecipient%
ex: `%SetRecipient%=mailbox@host.org`
Sets the address that will receive the auto-response message, regardless of the original sender.

%SetReplyTo%
ex: `%SetReplyTo%=mailbox@host.org`
Controls the value of the RFC-822 ReplyTo header

%SetActualTo%
ex: %SetActualTo%=mailbox@host.org
Changes who MDaemon thinks the "actual" recipient of the mail message should be.

%SetSubject%
ex: `%SetSubject%=Subject Text`
Replaces the value of the message's subject.

%SetMessageId%
ex: `%SetMessageId%=ID String`
Changes the ID string of the message.

%SetPartBoundary%
ex: `%SetPartBoundary%=Boundary String`
Changes what MDaemon thinks is the part boundary.

%SetContentType%
ex: `%SetContentType%=MIME type`
Changes what MDaemon thinks is the content-type of the message.

%SetAttachment%
ex: `%SetAttachment%=filespec`
Forces MDaemon to attach the specified file to the newly generated auto-response message.

Auto Response Script Samples

A typical auto response script might be called `VACATION.RSP` and look like this:

Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm on vacation so LEAVE ME ALONE!

Yours truly (yeah right!),

$RECIPIENT$

This is essentially the `VACATION.RSP` file that shipped with the first version of MDaemon. This example script uses macros developed for MBF files. Using the macros defined in the above table you can also control the headers which will be generated when this auto-response script is processed and mailed back to $SENDER$.

Let's amend our old `VACATION.RSP` file to use some of the new macros:

Greetings $SENDER$

You're message regarding '$SUBJECT$' won't be read by me because I'm on vacation so LEAVE ME ALONE!

Yours truly (yeah right!),

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\windows\bugoff.exe

The new message, which will be generated using this script as a template, will have a custom subject line and will have the specified file encoded as a MIME attachment.

The `%SetSubject%=RE: $SUBJECT$` instruction is handled in this way:

1. The `$SUBJECT$` portion is expanded and replaced by the original message's subject text. This makes the string equivalent to: `%SetSubject%=RE: Original Subject Text`.

2. MDaemon replaces the original subject, which it has stored in its internal buffers, with this newly calculated one. From then on any call to `$SUBJECT$` or use of the subject field will return the new result.

Note the placement of the new macros - they are listed at the bottom of the response script. This is needed to avoid side effects. For example, if the `%SetSubject%` macro were placed before the `$SUBJECT$` macro, which appears in the third line of the response script, the subject text will have been changed by the time the `$SUBJECT$` macro is expanded. Therefore, instead of replacing `$SUBJECT$` with the content of the original message's "Subject:" header, it will be replaced with whatever you have set the value of `%SetSubject%` to be.

Creating and Using MBF Files

MBF or Mailbox Format Files are text files designed to allow cross compatibility with other email transport systems that can accept ASCII text files into their mail streams. MBF files are essentially templates that contain a set of special formatting macros that enable MDaemon to transform an RFC-822 message into a variety of other text-based formats. Using MBFs, MDaemon can be configured to automatically reformat incoming mail into specific alternatives on a per mailbox basis. When a message arrives for an MDaemon account, the account's MBF file is used to reformat the incoming data before distributing it to the user.

MBFs are constructed as plain ASCII text files ending with the "`*.MBF`" file extension. They are scanned by the server for macros, which will be replaced by actual data from an incoming message. Lines beginning with the "#" character are ignored and are used for comments. Lines beginning with the ";" character are used to control the value of the reformatted message's file name. When the MBF processor sees a line that begins with the ";" character it assumes that the text following this character will describe either the prefix or the extension which the processor should use when creating new files.

The syntax is:

```
; msg-prefix = SMF<cr><lf>
; msg-ext = <cr><lf>
```

If an MBF file contained lines as shown above, all reformatted mail messages created using the MBF file would take the form "SMFxxxx" where "xxxx" represents a random but unique identifier. The maximum length of the prefix component is four characters. The maximum extension that can be specified is three characters. Note that the above example purposely excludes an extension. These directives are optional and are not required to be present in any MBF file. However, their inclusion provides a means of directly manipulating message file names, which may be useful in integrating **MDaemon Server v6** with an existing MTA. The default msg-prefix value is "MD" and the default msg-ext is "MSG".

Attachment file names can be similarly manipulated using the following syntax:

```
; attach-prefix = ATTH<cr><lf>
; attach-ext = ZIP<cr><lf>
```

This example would generate unique names for file attachments of the form “ATTHxxxx.ZIP” where “xxxx” represents a random yet unique identifier. Like those for message file names, these directives are optional.

> **Note**
>
> These directives will have no effect on accounts that are not auto-extracting embedded attachments.

It is sometimes important to retain the original file’s extension while generating a unique file name for it. To accomplish this use the “`; attach-ext = ???`” syntax. This causes MDaemon to retain the attachment’s original extension. By default, auto-extracted attachments are decoded and stored in the user’s FILES directory under their original file names.

MBF Macros and Examples

The following is a list of all macros available for use when constructing an MBF file. Following this list is a series of examples.

$HEADERS$

This macro will be replaced by all the original RFC-822 message headers - each separated by a CRLF delimiter. Using this macro the MBF will obtain all the headers contained in the incoming message. Text immediately preceding this macro will be duplicated at the start of each expanded line.

For example: O-SMTP-HEADER: $HEADERS$ would place each of the original RFC-822 headers into the reformatted message each preceded by the text string “O-SMTP-HEADER:”

$HEADER:XX$

This macro will cause the value of the header specified in place of the “xx” to be expanded in the reformatted message. For example: If the original message has “TO: joe@mdaemon.com” then the $HEADER:TO$ macro will expand to “joe@mdaemon.com”. If the original message has “Subject: This is the subject” then the $HEADER:SUBJECT$ macro would be replaced with the text “This is the subject”

$BODY$

This macro will be replaced by the entire message body. In an attempt to preserve character sets for different languages, MDaemon will read the message body as stream binary data rather than pure text, thus allowing a byte-for-byte copy of the message body.

$BODY-AS-TEXT$

This macro will be replaced by the entire message body as with the $BODY$ macro, except that MDaemon will read this as text rather than binary. This may not be compatible with all char sets. Text immediately preceding this template variable will be duplicated at the start of each expanded line; thus: >>$BODY-AS-TEXT$ would place each of the original RFC-822 message lines into the reformatted message with the addition of the string text “>>“ preceding them. Text could also be added to the right of this macro.

$ATTACHMENTS$

This macro will be replaced by the entire list of all attached files extracted from the original message. Text immediately preceding this template variable will be duplicated at the start of each expanded line; thus:
FILE-LIST $ATTACHMENTS$ would place each of the attachment file names into the reformatted message, each preceded by the text string “FILE-LIST”. NOTE: This macro is only available when you are extracting attachments from the account.

$ATTACHMENTCOUNT$

This macro will be replaced with an integer value equal to the number of attachments extracted from the original message. NOTE: This macro is only available when you are extracting attachments from the account.

$ATTACHMENT(X)$

This macro will be replaced with the attachment file name of the relative attachment number passed in the X parameter. If the value in X is greater than the total number of attached files then the entire variable is removed and replaced with nothing.

$SENDER$ This macro resolves to the full address of the message originator and corresponds to the RFC-822 “To:” header.

$SENDERMAILBOX$ This macro resolves to the mailbox of the message originator. The mailbox is the portion of the email address to the left of the “@” symbol.

$SENDERDOMAIN$ This macro resolves to the domain of the message originator. This is the portion of the email address to the right of the “@” symbol.

$RECIPIENT$ This macro resolves to the full address of the message recipient.

$RECIPIENTMAILBOX$ This macro resolves to the mailbox of the message recipient. The mailbox is the portion of the email address to the left of the “@” symbol.

$RECIPIENTDOMAIN$ This macro resolves to the domain of the message recipient. The domain is the portion of the email address to the right of the “@” symbol.

$SUBJECT$ This macro resolves to the value of the RFC-822 “Subject” header.

$MESSAGEID$ This macro resolves to the value of the RFC-822 “Message-ID” header.

$CONTENTTYPE$ This macro resolves to the value of the RFC-822 “Content-Type” header.

$PARTBOUNDARY$ This macro resolves to the value of the MIME “Part-Boundary” value found in the RFC-822 “Content-Type” header for multipart messages.

$DATESTAMP$ This macro expands to an RFC-822 style date-time stamp line.

$ACTUALTO$ Some messages may contain an “ActualTo” field which generally represents the destination mailbox and host as it was entered by the original user prior to any reformatting or alias translation.

$ACTUALFROM$ Some messages may contain an “ActualFrom” field which generally represents the origination mailbox and host prior to any reformatting or alias translation.

$REPLYTO$ This macro resolves to the value found in the RFC-822 “ReplyTo” header.

$PRODUCTID$ This macro expands to the **MDaemon Server v6** version information string.

\\XXX This variable specifies an ASCII character code (000 - 255) that should be inserted into the MBF file. This variable is always 5 characters long with the first two characters being “\\”. This instructs the server to expect a three digit number which represents an ASCII character code. For example, \\012 will place the ASCII character 12 (a formfeed character) into the MBF file. The numeric value specified must be three characters long and padded with zeros if necessary.

Sample MBF file(s):

1) RFC-822.MBF

```
# RFC-822.mbf - mailbox format for standard RFC-822 translations
# version 1.1
$HEADERS$
X-MBF-FILE: MDaemon Gateway to RFC-822 (RFC-822.MBF v3)

$BODY$
```

2) SMF70.MBF

```
# smf70.mbf - mailbox format for SMF minimal submission format
# version 1.1
; msg-prefix = SMF
; msg-ext =
SMF70
TO: $RECIPIENTMAILBOX$ @ $RECIPIENTDOMAIN$
FROM: $SENDER$
SUBJECT: $SUBJECT$
DATE: $DATESTAMP$
ATTACHMENT: $ATTACHMENTS$
O-SMTP-HEADER: $HEADERS$

$BODY$
```

3) DIGEST.MBF

```
# digest.mbf - default message format for digest mail
# version 1.0
Date: $HEADER:DATE$
From: $HEADER:FROM$
Subject: $HEADER:SUBJECT$

$BODY$
```

SECTION III

MDAEMON® VERSION 6

Additional MDaemon Features

Chapter

24

Mailing Lists

Using MDaemon's Mailing List Features.

Mailing Lists, sometimes called Email Groups or Distribution Lists, allow groups of users to be addressed as if they all shared a common mailbox. Copies of email messages sent to the list are distributed to each of the list's members. Lists may contain members with local and/or remote destination addresses, be public or private, moderated or open, be sent in Digest or normal message format, and more.

Mailing List Editor

The **Mailing List Editor** is used to create and maintain Mailing Lists and can be reached from the **Lists|New List…** or **Lists|Edit List…** menu selection.

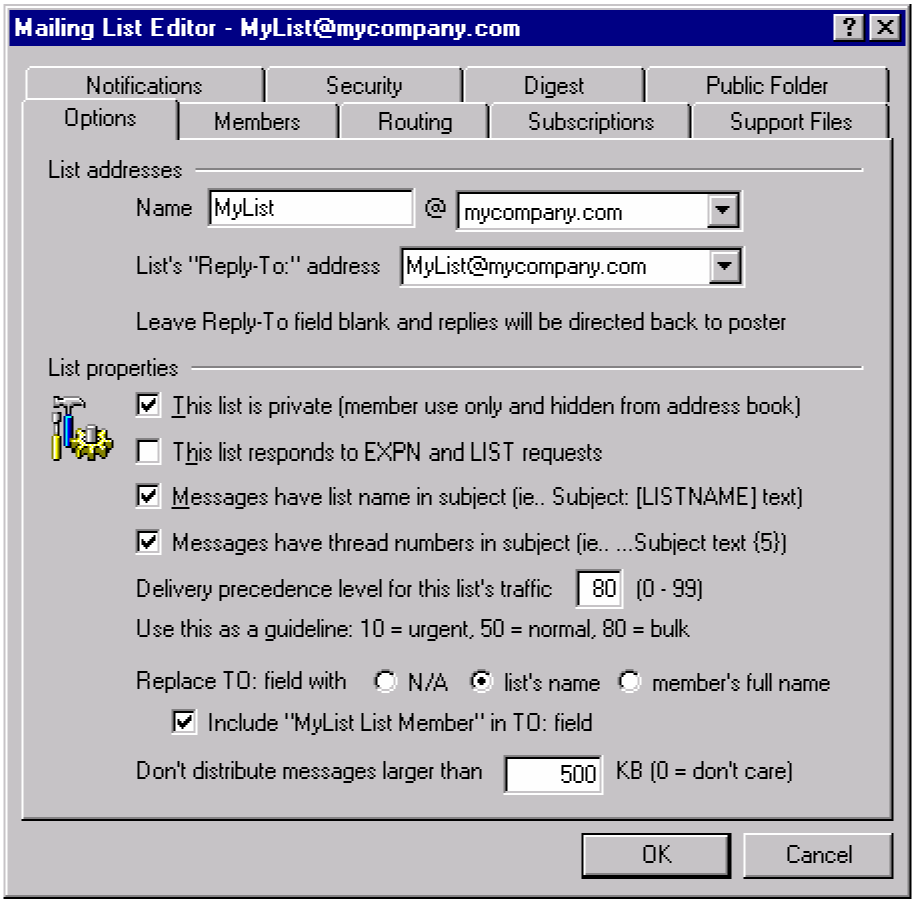
Creating a New Mailing List

When the **Lists|New List…** menu selection is chosen, the Mailing List Editor will be opened for creating the new list. Naming the list and designating the domain to which it will belong are the only required parameters for creating it. All other options will contain default settings. You can change these settings while creating the list or you can change them later by editing it.

Modifying an Existing Mailing List

Click the **Lists|Edit List…** menu selection to open the Select Mailing List dialog. This dialog is used to choose the Mailing List that you wish to edit. When a list is selected from this dialog it will be opened in the Mailing List Editor for editing or review.

Options



List addresses

Name: MyList @ mycompany.com

List's "Reply-To:" address: MyList@mycompany.com

Leave Reply-To field blank and replies will be directed back to poster

List properties

☑ This list is private (member use only and hidden from address book)

□ This list responds to EXPN and LIST requests

☑ Messages have list name in subject (ie.. Subject: [LISTNAME] text)

☑ Messages have thread numbers in subject (ie.. ...Subject text {5})

Delivery precedence level for this list's traffic: 80 (0 - 99)

Use this as a guideline: 10 = urgent, 50 = normal, 80 = bulk

Replace TO: field with ○ N/A ● list's name ○ member's full name

☑ Include "MyList List Member" in TO: field

Don't distribute messages larger than 500 KB (0 = don't care)

List Addresses

Name

Specify a name for the mailing list and then choose the domain to which the list will belong form the drop-down list box. Messages directed to this list will use the name and domain specified here (e.g. `mylist@mydomain.com`). List names cannot contain "!" or "|".

List's "Reply-To:" address

Type the email address to which you want replies to this list to be directed. Enter the list's address if you want replies to be directed back to it. You may enter an address other than the list name, or choose an address from the drop-down list if you want replies to this list to be directed to an alternate address. If you leave this field blank then replies to any list message will be directed back to the sender of that message.

List Properties

This list is private and only members can send list traffic

When this control is enabled, the list will only propagate messages from list members. Messages originating from non-members will be deleted.

This list responds to EXPN and LISTS requests

If this option is selected the membership of the list will be reported in response to an EXPN or LISTS command during a mail session. Otherwise, the list's membership will be kept private.

Messages have list name in Subject

This setting causes MDaemon to enclose the name of the list in brackets (e.g. [ListName]) and add it to the beginning of the `Subject:` in all messages sent to the list.

Messages have thread numbers in Subject (ie…Subject text {5})

This switch allows you to toggle whether thread numbers will be displayed in the `Subject:` header of list messages. They are appended to the end of the subject line in braces and used as a pseudo-thread number. Sorting your inbox by subject will align list mail in chronological order.

Delivery precedence level for this list's traffic

Enter a number from 0-99 in this control. This value signifies the relative sort order of the messages during the delivery process. The lower the value, the higher its importance and the further up it will be in the sort order within a message queue. As a guideline for assigning values: 10 = Urgent, 50 = Normal, and 80 = Bulk.

Replace 'TO:' field with: N/A, list's name, member's full name

Use these options to designate what address will be displayed in the TO: field whenever MDaemon receives a message directed to the list.

N/A - When **N/A** is selected MDaemon will make no changes to the address displayed. The address contained in the TO: field will appear exactly as the sender of the message entered it.

List's name - This option displays the address of the Mailing List in the 'TO:' field.

Member's full name - When this option is selected, the 'TO:' field will contain the full name and email address of the list member to whom the message is directed, or just the email address if the full name is not available.

Note

The Member's Name option can only be chosen when "*MDaemon Will Crack List Mail*" has been selected on the Routing tab of the Mailing List Editor. When "*Route A Single Copy…*" is selected, MDaemon will default to the List's Name option.

Include "[Listname] List Member" in TO: field

When this feature is enabled, "[Listname] List Member" will be displayed in the "real name" portion of the message's TO: field.

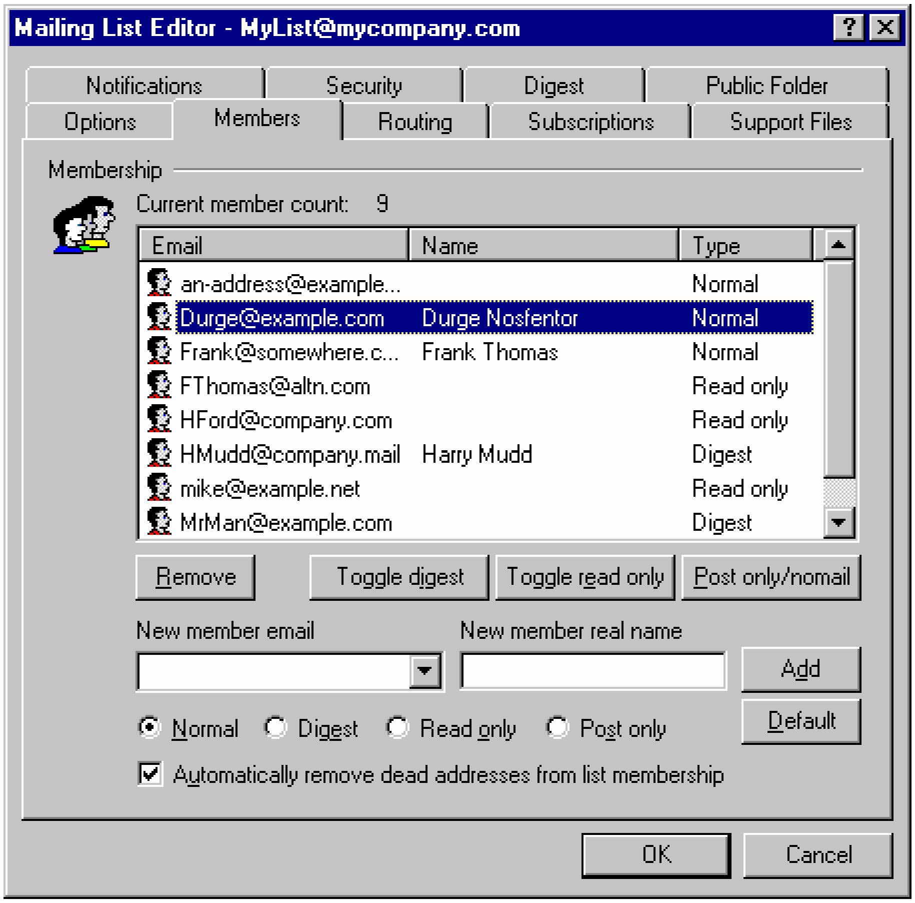
Note

Not all email clients support the displaying of "real names" in the TO: field of messages. In such clients only the actual email address designated in the "*Replace TO: Field With…*" feature will appear.

Don't distribute messages larger than XX bytes

This control places an upper limit on the size of a message accepted for this mailing list. Messages larger than this limit are sent to the bad message directory.

Members



Current member count: 9

Email	Name	Type
an-address@example...		Normal
Durge@example.com	Durge Nosfentor	Normal
Frank@somewhere.c...	Frank Thomas	Normal
FThomas@altn.com		Read only
HFord@company.com		Read only
HMudd@company.mail	Harry Mudd	Digest
mike@example.net		Read only
MrMan@example.com		Digest

● Normal ○ Digest ○ Read only ○ Post only

☑ Automatically remove dead addresses from list membership

Membership

Current member count:
This control displays the current number of users subscribed to the list and lists them in the box below. Each member's entry also states his or her "type" of membership: normal, digest, read only, or post only.

Remove
This button removes the selected entries from the *Current Members* list.

Digest
Select a member and then click this button to make it a "Digest" membership. See **Digest** (page 283) for more information on Digest mail.

Read only
Click this button after selecting a list member to give their membership "Read Only" status. They will still receive messages from the list but will not be allowed to send them to it.

Post only/no mail
Clicking this button after selecting a member will set their membership to "Post Only". They will be allowed to send messages to the list but will not receive any.

New member email

Enter the email address of the person you wish to add to the mailing list. Member's addresses cannot contain "!" or "|".

New member real name

Enter the member's name in this field. This name will appear in the "To:" field of their list messages when the "*Replace 'TO:' field with: member's full name*" option is selected on the Options tab.

Normal, Digest, Read only, Post only

Click the option that you want to be applied to the *New Member's Email Address.*

Add

This button adds the entry in the *New Member's Email Address* control to the *Current Members* list.

Default

Click any one of the options next to this button (*Normal, Digest, Read Only, Post Only*) and then click the button to make that option the default setting for new members.

Automatically remove dead addresses from list membership

When this feature is enabled, MDaemon will automatically remove an address from the *Members* list when it encounters a permanent fatal error while attempting delivery. Addresses will also be considered "dead" and removed when their message is moved to the Retry system and subsequently expires from that system.

Note

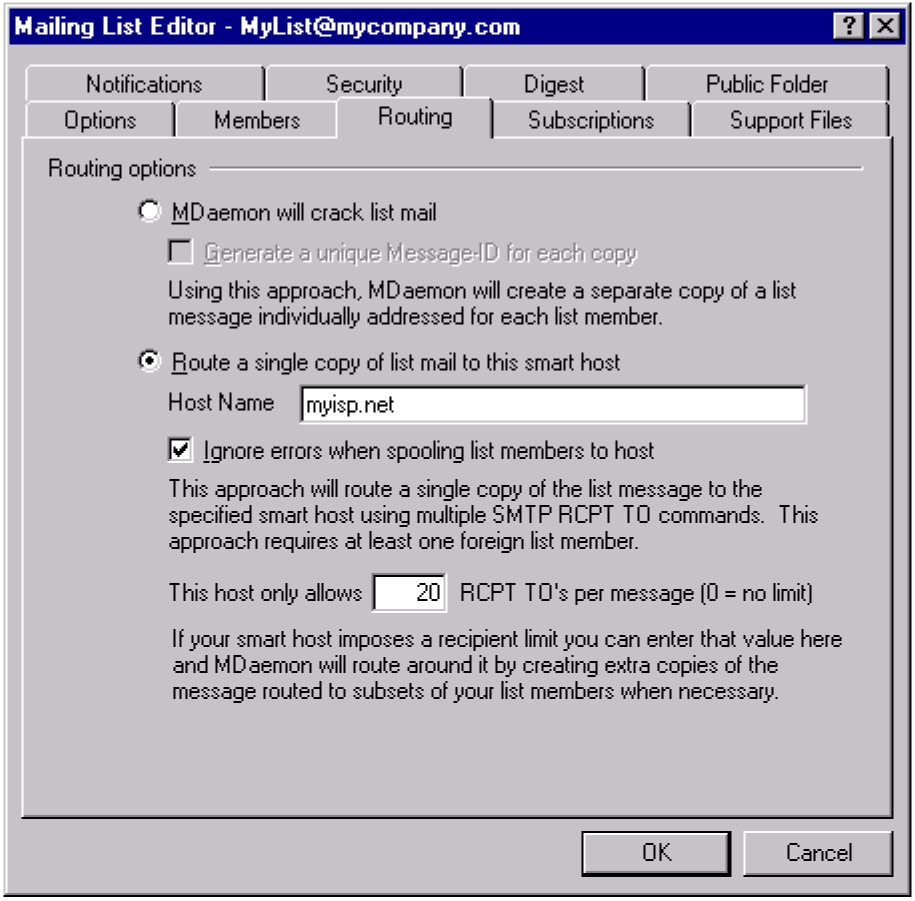
The *Automatically remove dead addresses…* switch is only designed to assist in situations where the remote mail server refuses to accept messages. This will only work when you have configured MDaemon to crack the mailing list (page 273) and not use a smart host. If you are routing list messages to a smart host then see Enhanced List Pruning below for more information.

Enhanced List Pruning

When the *Automatically remove dead addresses…* control is enabled and you have specified a local mailbox as the return path for the list's messages (see the Returned Mail control on the Notifications tab), each day at midnight MDaemon will attempt to parse problem addresses from the returned mail and remove those members that couldn't be reached. This will aid in more efficiently pruning invalid addresses from mailing lists, especially when you are routing the list's messages to a smart host rather than delivering them directly.

On the Misc tab of Miscellaneous Options (page 210) there are two controls related to this feature. One of them will cause returned messages that do not contain a parsable address to be deleted. The other will cause all messages that result in a list member being deleted to be saved.

Routing



Mailing List Editor - MyList@mycompany.com

Routing options

○ MDaemon will crack list mail

□ Generate a unique Message-ID for each copy

Using this approach, MDaemon will create a separate copy of a list message individually addressed for each list member.

● Route a single copy of list mail to this smart host

Host Name: myisp.net

☑ Ignore errors when spooling list members to host

This approach will route a single copy of the list message to the specified smart host using multiple SMTP RCPT TO commands. This approach requires at least one foreign list member.

This host only allows 20 RCPT TO's per message (0 = no limit)

If your smart host imposes a recipient limit you can enter that value here and MDaemon will route around it by creating extra copies of the message routed to subsets of your list members when necessary.

MDaemon will crack list mail

If selected, individual list messages will be created and dispatched to each list member. This will result in numerous individual messages being created which could affect the server's performance. This option is appropriate for a mailing list of around 15 members or less.

Generate a unique Message ID for each copy

When MDaemon cracks list mail it creates an individual copy of the message for each member. If you wish, MDaemon can make certain that each copy of the list message contains a unique identifier.

Route single copy of list mail to this smart host | Host Name

If selected, MDaemon will route a single copy of each list message to the specified smart host. This method employs multiple RCPT TO commands during the SMTP session with the specified host.

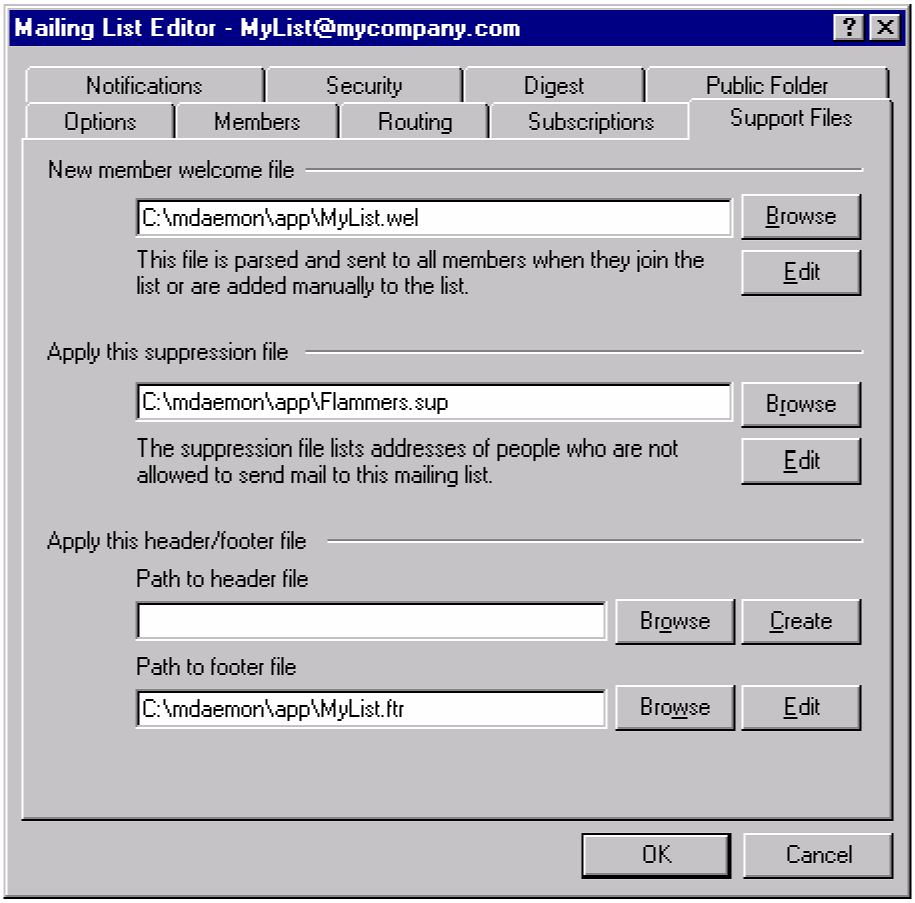
Ignore errors when spooling list mail to host

Since some smart hosts will refuse to queue or spool mail for certain domains, the routed approach to list delivery could cause numerous problems. An error code returned from the smart host as a result of this refusal would ordinarily cause MDaemon to abort the delivery attempt. If this switch is set MDaemon will ignore error codes returned from the smart host during delivery of routed list mail thus allowing those members that are accepted a chance to receive the list message.

This host allows [XX] RCPT TO's per message (0=no limit)

Some hosts limit the number of RCPT TO statements that they will accept when you are attempting to route a single copy of a message through them. If you specify the limit in this control then MDaemon will work around it by creating additional copies of the message and dividing the list into smaller groups. Then it will deliver the message to those groups thus avoiding the need to exceed the limitation. This is similar to "cracking" the list, but into groups instead of individuals.

Support Files



New member welcome file

C:\mdaemon\app\MyList.wel

This file is parsed and sent to all members when they join the list or are added manually to the list.

Apply this suppression file

C:\mdaemon\app\Flammers.sup

The suppression file lists addresses of people who are not allowed to send mail to this mailing list.

Apply this header/footer file

Path to header file

Path to footer file

C:\mdaemon\app\MyList.ftr

New Member Welcome File

If specified, the file listed here will be processed and mailed to all new members just after they subscribe. The file is processed and handled exactly the same way as Auto-Response scripts and may therefore contain any macro available to them.

See:

Creating Auto Response Scripts - page 261

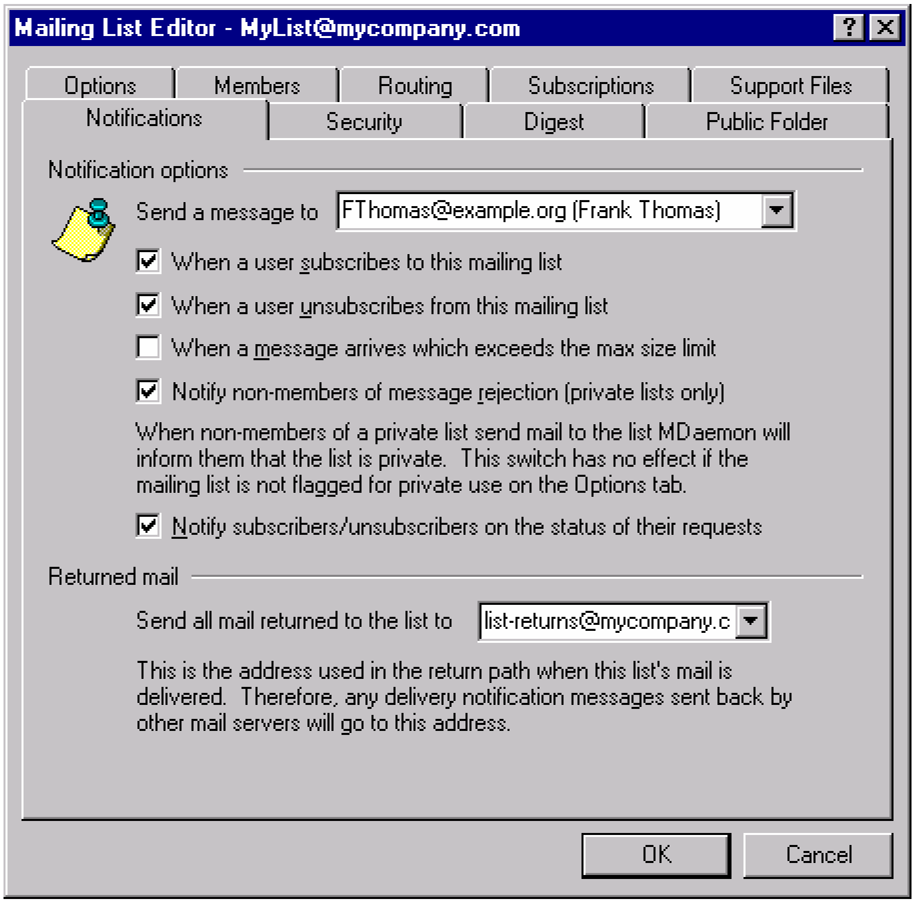
Apply This Suppression File

If specified, the file listed here will be used to suppress messages sent from specified users. For a discussion on suppression files see **Address Suppression**—page 109.

Apply This Header/Footer File

The contents of the files specified here will be used as the header and/or footer file for list messages.

Notifications



Mailing List Editor - MyList@mycompany.com

Send a message to: FThomas@example.org (Frank Thomas)

☑ When a user subscribes to this mailing list

☑ When a user unsubscribes from this mailing list

□ When a message arrives which exceeds the max size limit

☑ Notify non-members of message rejection (private lists only)

When non-members of a private list send mail to the list MDaemon will inform them that the list is private. This switch has no effect if the mailing list is not flagged for private use on the Options tab.

☑ Notify subscribers/unsubscribers on the status of their requests

Send all mail returned to the list to: list-returns@mycompany.c

This is the address used in the return path when this list's mail is delivered. Therefore, any delivery notification messages sent back by other mail servers will go to this address.

Notification Options

Send a message to
This control lists an address that will be notified when the selected events take place.

When a user subscribes to this mailing list
If selected, a note will be sent to the address specified in the associated control each time someone subscribes to the mailing list.

When a user unsubscribes to this mailing list
If selected, a note will be sent to the address specified in the associated control each time someone unsubscribes to the mailing list.

When a message arrives which exceeds the max size limit
If selected, a note will be sent to the address specified in the associated control each time someone sends a message to the mailing list that is larger than the maximum acceptable size. Such messages are moved into the bad message directory.

Notification Options

Notify non-members of message rejection (private lists only)

When non-members of a private list send mail to the list, MDaemon will inform them that the list is private. They will also be given instructions on how to subscribe to lists.

Notify subscribers/unsubscribers on the status of their requests

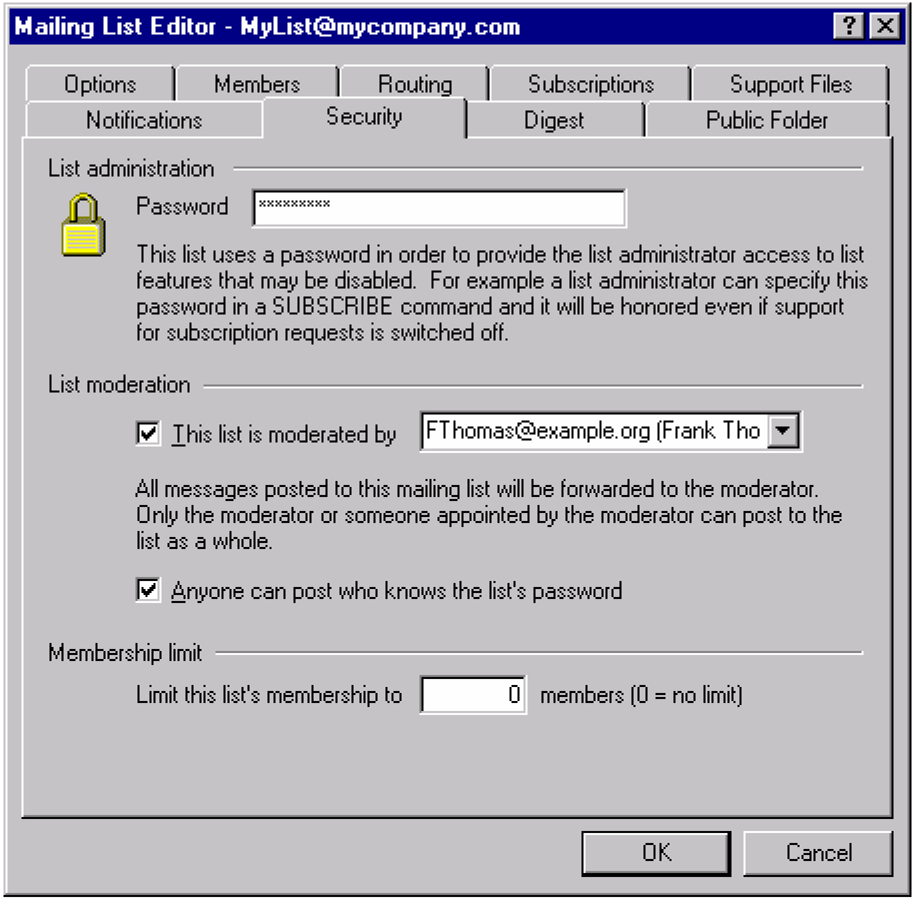
When this checkbox is enabled MDaemon will send a completion notification message to the user that has been subscribed/unsubscribed to the Mailing List.

Returned Mail

Send all mail returned to the list to

Here you specify who should receive any returned mail generated from list traffic. For example, a mailing list with 100 recipients will generally have 10-20 undeliverable addresses either due to address changes or down servers or whatever. The SMTP system will generate and return to the sender of the message notification mail concerning these undeliverable conditions. You can configure who should receive these messages for your mailing lists. You can also specify that no one should receive them in which case MDaemon will place list mail into the mail stream in such a way that return mail will not be possible.

Security



List administration

Password: **********

This list uses a password in order to provide the list administrator access to list features that may be disabled. For example a list administrator can specify this password in a SUBSCRIBE command and it will be honored even if support for subscription requests is switched off.

List moderation

☑ This list is moderated by: FThomas@example.org (Frank Tho

All messages posted to this mailing list will be forwarded to the moderator. Only the moderator or someone appointed by the moderator can post to the list as a whole.

☑ Anyone can post who knows the list's password

Membership limit

Limit this list's membership to: 0 members (0 = no limit)

List Administration

Password
Enter the lists access password in this control.

List Moderation

This list is moderated by
If set, the list will be moderated by the specified user. Moderated lists forward all posts to the moderator. The moderator alone may submit or forward messages to the list.

Anyone can post who knows the list's password
If this option is checked the moderator can assign a password to the mailing list. Messages submitted to a moderated list that have the appropriate password specified as the first X characters of the subject line will not be subject to moderation - that is, the message will be immediately posted as if it had come from the moderator.

For example: to bypass the moderator on a moderated list called MDSUPP, which has a password of ALTN, make ALTN the first 4 characters of the message subject.

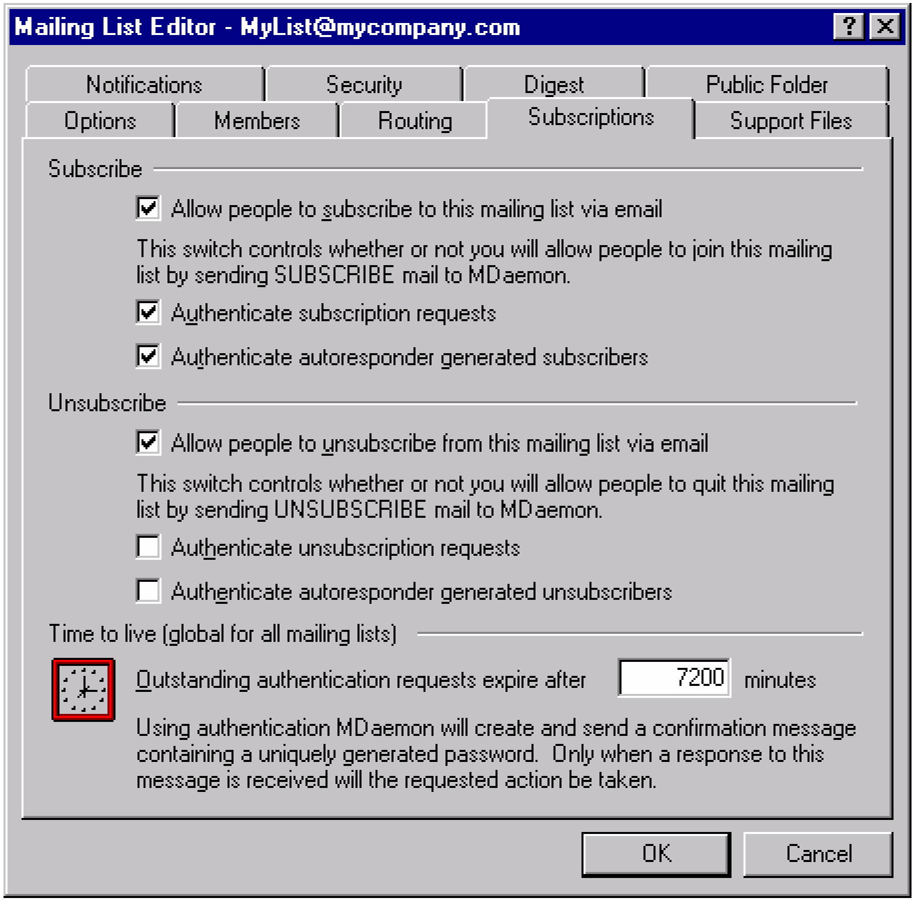
Membership limit

Limit this list's membership to [xx] members (0=no limit)
With this feature you can place an upper limit on the number of people who are allowed to subscribe to the Mailing List. Enter a zero into this field if you do not wish to limit list subscriptions.

Note

This limit is only placed upon those who can Subscribe to the list through the Subscribe command. This limit does not apply to subscriptions entered through the MDaemon interface, or through Subscription commands that are accompanied by the list Password.

Subscriptions



Subscribe

☑ Allow people to subscribe to this mailing list via email

This switch controls whether or not you will allow people to join this mailing list by sending SUBSCRIBE mail to MDaemon.

☑ Authenticate subscription requests

☑ Authenticate autoresponder generated subscribers

Unsubscribe

☑ Allow people to unsubscribe from this mailing list via email

This switch controls whether or not you will allow people to quit this mailing list by sending UNSUBSCRIBE mail to MDaemon.

□ Authenticate unsubscription requests

□ Authenticate autoresponder generated unsubscribers

Time to live (global for all mailing lists)

Outstanding authentication requests expire after 7200 minutes

Using authentication MDaemon will create and send a confirmation message containing a uniquely generated password. Only when a response to this message is received will the requested action be taken.

Subscribe

Allow people to subscribe to this mailing list via email

This switch controls whether or not the list will allow potential members to subscribe to the mailing list by sending a subscription request to MDaemon.

Authenticate subscription requests

With this switch set MDaemon will attempt to authenticate the subscription request. The mechanism employed to accomplish this consists of MDaemon generating a unique password string for the subscription transaction. A message is sent to the potential member which contains this unique password. Once the potential member responds by replying to this message MDaemon will then add the member to the mailing list's membership.

Authenticate autoresponder generated subscribers

Click this option if you want authentication to be required when the member is added via the *Add Sender to This Mailing List* Auto responder feature (page 259).

Unsubscribe

Allow people to unsubscribe from this mailing list via email

This switch controls whether or not the list will allow members to quit the mailing list by sending an unsubscription request to MDaemon.

See:

Remote Server Control Via Email - page 318

Authenticate unsubscription requests
With this switch set MDaemon will attempt to authenticate the unsubscription request. See *Authenticate Subscription Requests* for a discussion of the mechanism employed to accomplish this.

Authenticate autoresponder generated unsubscribers
Click this option if you want authentication to be required when the member is removed via the *Remove Sender From This List* Auto responder feature (page 259).

Time to Live (global for all mailing lists)

Outstanding authentication requests expire after XX minutes
When someone is subscribed or unsubscribed, this is the amount of time that they have to confirm the subscription command before it will be discarded. MDaemon will generate a confirmation message and send it the subscribed address. The recipient must reply to the message within the designated time limit before the subscription command will be considered valid. This value is global; it applies to all MDaemon mailing lists not just the one that is currently being edited.

Subscribing To Mailing Lists

To subscribe to a mailing list, send an email message addressed to `MDaemon` (or any alias thereof) at the domain hosting the mailing list, and place the `Subscribe` command as the first line of the message body. For example, there is a mailing list called `MD-Support` being hosted by `altn.com.` You can subscribe to the list by composing a message addressed to “`mdaemon@altn.com`” and placing the value: `SUBSCRIBE MD-Support@altn.com` as the first line of the message body. The message subject is irrelevant and can be left blank.

For complete details on how to form this and other control messages, see:

Remote Server Control via Email - page 318

You can also utilize MDaemon’s Auto Responder features to automatically subscribe members to a list when they send messages to an auto-responder enabled account. See page 259 for details on this feature.

Finally, new to MDaemon version 6 is a subscription feature that can be used to cause MDaemon to recognize email addresses of the formats “`[list]-subscribe@domain.com`” and “`[list]-unsubscribe@domain.com`” (as long as the list actually exists) in order to facilitate an easier method for users to join and leave your mailing lists. For example: suppose you have a list called `MyList@altn.com`. People will be able to subscribe/unsubscribe to your list by sending an email message to `MyList-Subscribe@altn.com` and `MyList-Unsubscribe@altn.com`. The content of the subject and message body is irrelevant. Also, when this feature is active MDaemon will insert the following header into all list messages:

```
List-Unsubscribe: <mailto:<List>-Unsubscribe@domain.com>
```

Some mail clients can pick up on this and make an UNSUBSCRIBE button available to users automatically.

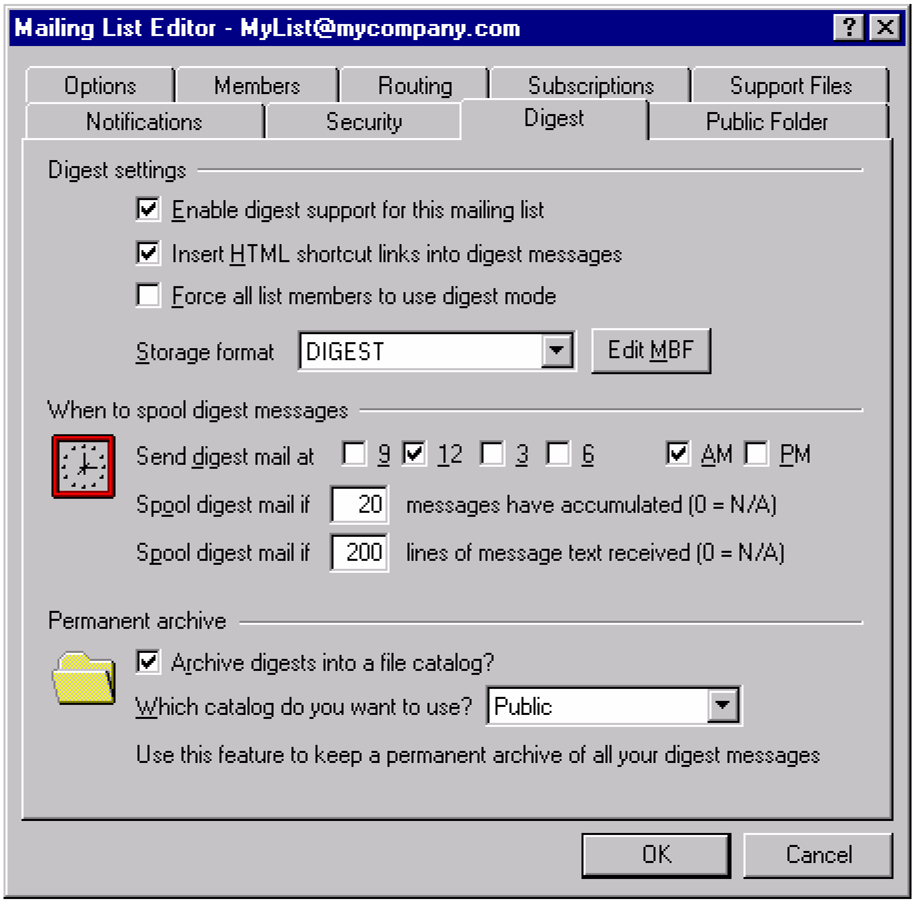
This new feature is located on the Misc tab of Miscellaneous Options (page 210).

Note

Occasionally, users will attempt to subscribe/unsubscribe to lists via email by sending the commands to the list itself rather than to the MDaemon system account. This results in the command being posted to the list rather than the user being subscribed or unsubscribed. To prevent these sorts of messages from being posted to mailing lists, enable the *Pre-process mailing list mail* control on the System tab of Miscellaneous Options (page 203).

This will cause messages containing subscribe, unsubscribe, and signoff commands in the first line of the message body to be rejected when those commands contain the list name and are sent to the list's address rather than the system account.

Digest



Digest settings

☑ Enable digest support for this mailing list

☑ Insert HTML shortcut links into digest messages

☐ Force all list members to use digest mode

Storage format DIGEST

When to spool digest messages

Send digest mail at ☐ 9 ☑ 12 ☐ 3 ☐ 6 ☑ AM ☐ PM

Spool digest mail if 20 messages have accumulated (0 = N/A)

Spool digest mail if 200 lines of message text received (0 = N/A)

Permanent archive

☑ Archive digests into a file catalog?

Which catalog do you want to use? Public

Use this feature to keep a permanent archive of all your digest messages

Digest Settings

Enable digest support for this mailing list

This control determines whether this mailing list support message digests. When digest support is enabled, a copy of each message sent to the mailing list will be archived. Members of the mailing list who have elected to receive traffic from this list in digest form will be sent these archived messages in a compact and easy to use indexed format.

Insert HTML shortcut links into digest messages

When this control is enabled, MDaemon will convert all URLs found within digest messages to hypertext links.

Force all members to use digest mode

By default, list members can control whether they wish to receive list traffic in digest or regular format. This control forces all members to use digest mode irrespective of the mode they may have chosen for themselves.

Storage format

Select the MBF file that individual messages placed into the digest will be conformed to. The default `DIGEST.MBF` file provides typical functionality comparable to most other mailing list software. For complete details on how to create MBF files see **Creating and Using MBF Files**—page 263.

Edit MBF
Click this button to edit the Mailbox Format file listed in the *Storage format* control.

When to Spool Digest Messages

Send digest mail at 9, 12, 3, 6 am and/or pm
Mailing list digests must periodically be sent to those list members who are set to receive mail in digest format. These controls allow you to configure when you wish MDaemon to do this.

Spool digest mail if [XX] messages have accumulated (0 = N/A)
Sometimes digests should be sent to list members based upon the number of messages that have accumulated rather than (or in addition to) specific times. This control allows you to specify the number of messages that the list will accumulate before sending the digests to digest mode list members.

Spool digest mail if [XX] lines of message text received(0 = N/A)
This control will cause Digest mail to be sent immediately when a digest grows to this many lines of text.

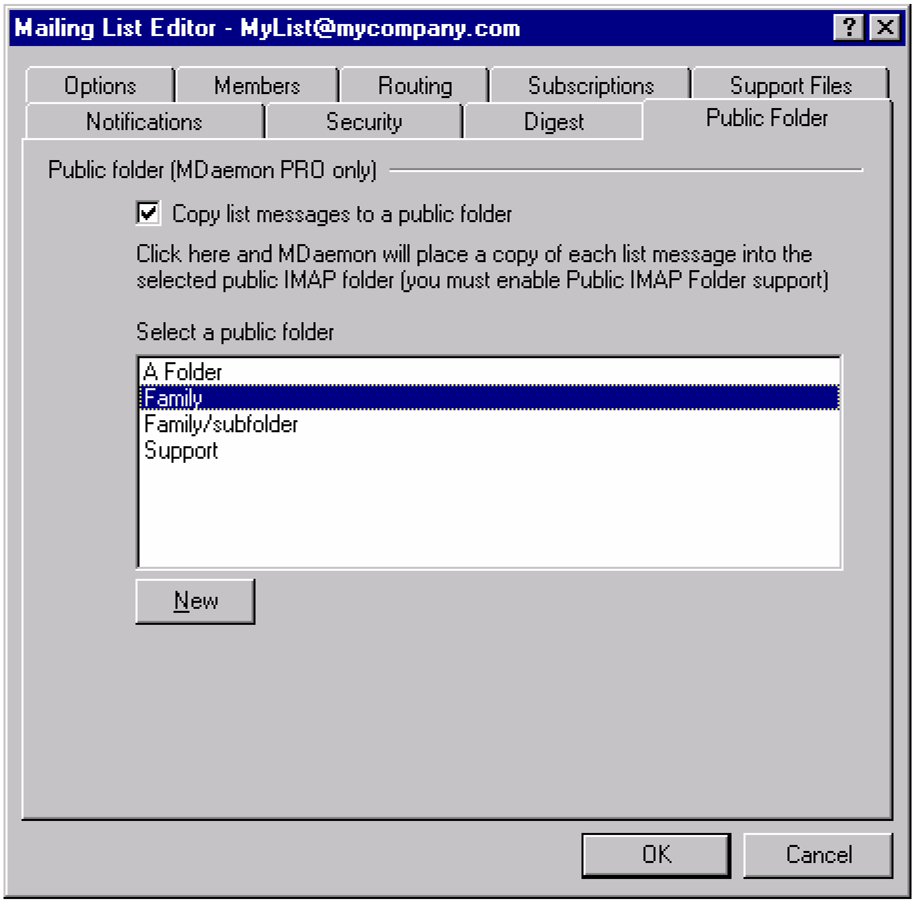
Permanent Archive

Archive digests into a file catalog / which catalog do you want to use?
These controls allow you to place digest messages into a file catalog so that back-issues of the digests can be collected in the future. MDaemon will generate a unique archive name for each digest and place it into the catalog you specify.

For complete information on how to work with catalogs see:

Creating A New Catalog—page 286

Public Folder



Public folder (MDaemon PRO only)

☑ Copy list messages to a public folder

Click here and MDaemon will place a copy of each list message into the selected public IMAP folder (you must enable Public IMAP Folder support)

Select a public folder

- A Folder
- Family
- Family/subfolder
- Support

New to this version of MDaemon is support for Public IMAP Folders. Public folders are extra folders that are available to multiple IMAP users, unlike personal IMAP folders, which are typically only accessible by a single user. The controls on this tab are used to cause all messages destined for this Mailing List to be automatically copied to one of your public folders. For more information on Public Folders see page 102.

Public Folder

Copy list messages to a public folder

Enable this control if you want this list's messages to be copied to one of your Public Folders in addition to being delivered to the list as usual.

Select a public folder

Click the Public Folder that you wish to associate with this list's messages.

New

Click the *New* button if you wish to create a new Public Folder for use with this list. This will cause the Public Folders dialog (page 102) to be opened.

Chapter

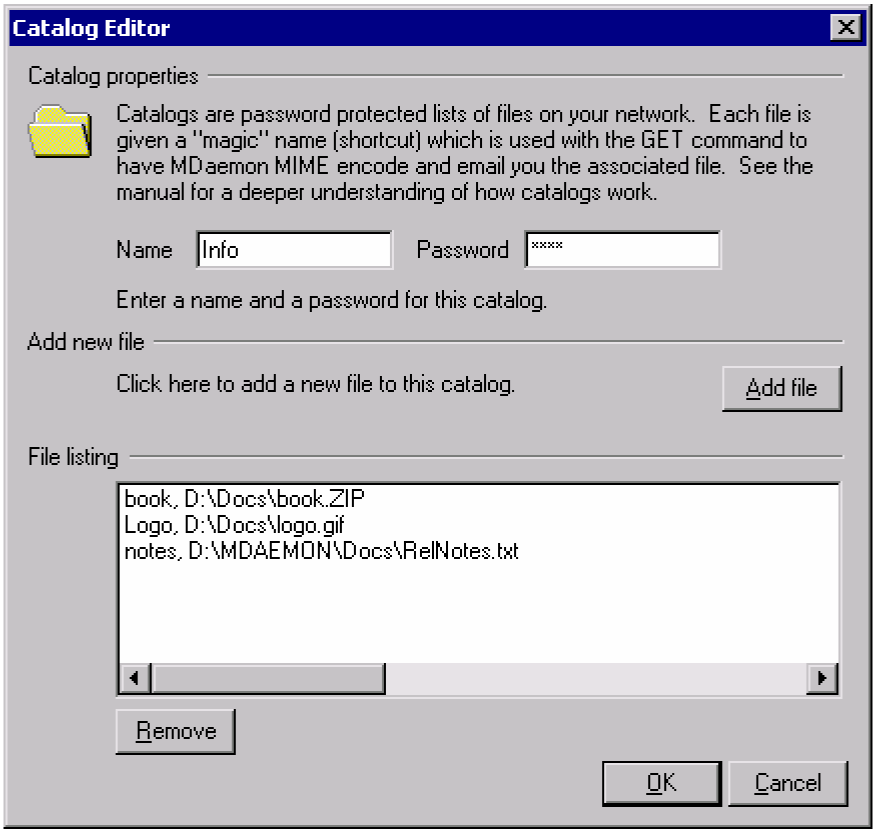
25

Catalogs

Utilizing MDaemon's Catalogs feature.

Use the **Catalogs|New Catalog…** or **Catalogs|Edit Catalog…** menu selection to open the Catalogs Editor for creating or editing a file catalog. Catalogs give users the ability to request files across the network and have them encoded and mailed back to them. Catalogs work by allowing the mail administrator to assign "magic names" (shortcuts) to files on disk. Magic names are like aliases which point to a specific file located somewhere accessible to MDaemon. A user can then use a special type of email message to request the file using the magic name. The format of this special email message is described in the **Remote Server Control** section (see the **GET** command in **Mailing List and Catalog Control**—page 319).

Catalog Editor



Catalogs are password protected lists of files on your network. Each file is given a "magic" name (shortcut) which is used with the GET command to have MDaemon MIME encode and email you the associated file. See the manual for a deeper understanding of how catalogs work.

Name: Info

Password: ****

Enter a name and a password for this catalog.

Click here to add a new file to this catalog.

book, D:\Docs\book.ZIP
Logo, D:\Docs\logo.gif
notes, D:\MDAEMON\Docs\RelNotes.txt

Catalog Properties

Name

Use this field to enter a name for the file catalog.

Password
Use this field to enter a password for the file catalog.

> **Note**
>
> Since MDaemon v3, a password is no longer required for all catalogs. You may choose to make catalogs accessible without a password.

See:

Mailing List and Catalog Control - page 319

Add New File

Add file
Click this button to add a file to the catalog. After choosing the file that you wish to add you will be prompted for the "Magic name" that you wish to assign.

File Listing

This window displays all the files and their associated "magic names" currently registered as members of the specified catalog. Double click on an entry in this window to remove it from the catalog.

Remove
Click this button to remove a selected entry from the *File Listing*.

The PUBLIC Catalog

The PUBLIC catalog is an exception to the normal rules governing access to file catalogs. Typically, to access a catalog requires a password that has been assigned to the catalog. With the PUBLIC catalog the password is not required. Files listed in the PUBLIC catalog are available to anyone who knows the file's magic name.

Chapter

26

Domain Gateways

Adding and configuring domains for which MDaemon will act as a Gateway.

The Gateway Editor is reached by clicking the **Gateways|New Gateway…** or **Gateways|Edit Gateway…** menu selection on the Message Router. This feature provides a limited yet useful secondary level of support for hosting multiple domains. When a message arrives for a domain for which MDaemon is acting as a gateway, it is separated from the main mail stream and delivered to the directory specified for it in the Gateway Editor. Additionally, attachments can be automatically extracted and placed in the specified attachment directory. Further, all mail is re-formatted according to its specified MBF file. You can host as many domains as you like using this method.

An example will prove useful here:

> Suppose you want to "partially" host a domain for another department. You want to collect its mail and deposit it in a directory but do not want to maintain its accounts on your server. Let's use "`company.com`" as its name. The first thing you will do is enter "`company.com`" in the *Domain Name* field on the Domain Settings tab of the Editor. Then, you will select and enter the disk directory where incoming mail messages and file attachments should be stored. You don't have to use the auto-extraction of attachments feature unless it is needed. Finally, either select an existing MBF file or install a new one. The default RFC-822 MBF file will ensure that all mail stored for "`company.com`" will be in RFC-822 format. Once all the settings have been entered click *Apply* or *Ok*.
>
> Now that the domain "`company.com`" has been installed as a client domain, MDaemon will store all messages that it receives for that domain in the directory specified, and in the format you have dictated—regardless of to whom the messages are directed. In other words, **all mail** for that domain will be pooled into a single directory on disk. You will setup this directory and a POP account for the domain to access directly from the Gateway Editor by entering a name and password on the Gateway Editor's *POP Access* tab and then clicking the *Create/Update Account* button. All that remains is for the domain to collect its mail from MDaemon via its POP account. This can be done by either a mail client or another MDaemon, which could utilize its DomainPOP feature to further distribute the mail to the domain's users (as would be the case in our example). Alternatively, you can use the controls on the ESMTP ETRN and ATRN/AUTH tabs so that the domain could collect and distribute its mail to its users via ESMTP instead of POP or DomainPOP.

This all works perfectly for LAN and WAN based systems that can easily be configured to resolve an arbitrarily assigned domain name like the "`company.com`" example. However, how can Internet email support be provided for "`company.com`" if the domain doesn't really exist on the Internet? There are two ways to cope with this problem. First, the domain can be registered with the Internet authorities and configured to resolve to the same IP address as the MDaemon that you want to collect its mail. Better yet, it can be registered as an alias to the primary domain name. Failing this, a message can still be delivered by "hiding" "`company.com`" within a primary domain address. Using this method addresses can be constructed that will pass through the primary domain and on to the users of the domain for which MDaemon is acting as a gateway. For example, if an outside Internet mail user wishes to send a message to "`bob@company.com`", which is domain gateway served by "`mydomain.com`", then the sender would need to address his email message to "`bob{company.com}@mydomain.com`". Because "`mydomain.com`" is a registered domain hosted by MDaemon, this message will be delivered properly. When MDaemon receives a message with an address in this format it will convert the address to "`bob@company.com`" and deliver the message to the disk directory specified for that domain.

Gateway Editor

The *Gateway Editor* includes the following tabbed dialogs:

Domain settings
This dialog contains the domain name of the particular domain that you are working with, as well as the path to the directory used for storing messages and file attachments addressed to this domain. Here you will also assign an MBF file to be used when MDaemon delivers mail to this domain's mailbox.

ESMTP ETRN
Use the controls on this dialog to choose whether MDaemon will respond to ESMTP ETRN requests made on behalf of the domain in order to dequeue its messages. To aid in security, this dialog also contains controls that make it possible to assign specific IP addresses that MDaemon will honor these requests from, or you can designate IP addresses that will be ignored.

ATRN / AUTH
Use the controls on this tab if you want MDaemon to respond to `ATRN` commands from the domain for which MDaemon is acting as an email gateway. The tab also contains controls for specifying the domain's shared secret necessary for authentication and for designating whether or not authenticated requests should be considered valid regardless of IP address.

Mail forwarding
With this dialog you can declare a host to which the domain's mail will be forwarded as soon as it arrives. There is also a control for stating whether a copy of these messages will be kept locally.

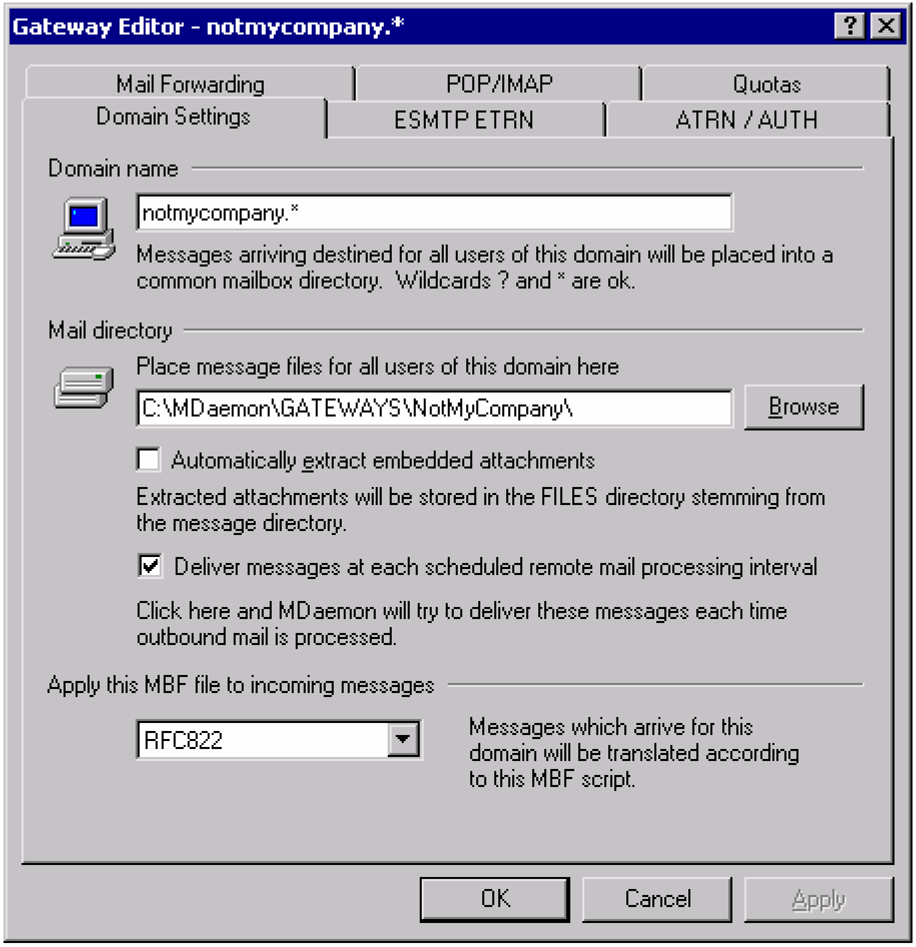
POP/IMAP
Here you can create a POP account that will have access to this domain's stored mail. Using the name and password that are assigned here, an ordinary mail client or another MDaemon installation can access the domain's mailbox and collect its mail.

Quotas
This dialog is used for assigning a limit to the amount of disk space that the domain may use and the maximum number of messages that may be stored.

Automatic Gateways Creation

The controls on this dialog (Gateways→Automatic Gateway Creation...) are used to configure MDaemon to automatically create a Domain Gateway (page 289) for a previously unknown domain when another source attempts to deliver that domain's messages to MDaemon, and a DNS query lists MDaemon's location as a valid MX record.

Domain Settings



Gateway Editor - notmycompany.*

Domain name

notmycompany.*

Messages arriving destined for all users of this domain will be placed into a common mailbox directory. Wildcards ? and * are ok.

Mail directory

Place message files for all users of this domain here

C:\MDaemon\GATEWAYS\NotMyCompany\

□ Automatically extract embedded attachments

Extracted attachments will be stored in the FILES directory stemming from the message directory.

☑ Deliver messages at each scheduled remote mail processing interval

Click here and MDaemon will try to deliver these messages each time outbound mail is processed.

Apply this MBF file to incoming messages

RFC822

Messages which arrive for this domain will be translated according to this MBF script.

Domain Name

Enter the name of the domain for which you wish MDaemon to act as an email gateway.

Mail Directory

Place message files for all users of this domain here
Enter the directory where you want to store incoming mail for the domain.

Automatically extract embedded attachments
Some mail systems require attached files be extracted before submission of mail messages to the mail stream. To facilitate this, MDaemon can auto-extract incoming MIME attachments and place them in the `\Files\` subdirectory underneath the domain's message directory. This directory will only be used if the "Auto-Extract" switch is selected.

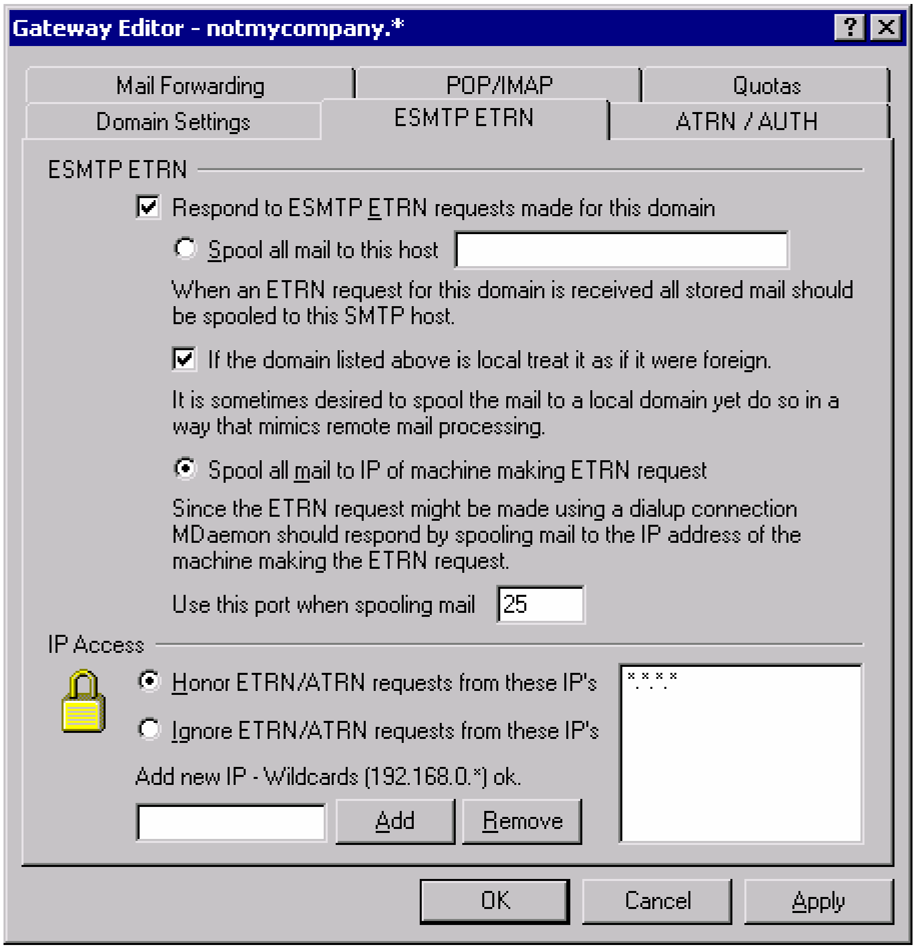
Deliver messages at each scheduled remote mail processing interval
Ordinarily, when MDaemon receives mail that is intended for one of its Domain Gateways it will store the messages until in that domain connects to MDaemon to collect it. In some situations you may want MDaemon to attempt to deliver the mail directly via SMTP rather than waiting for the domain to collect

it. When this control is enabled, MDaemon will attempt to deliver the domain's messages at each remote mail processing interval. The gateway's mailbox will temporarily act as a remote queue and delivery will be attempted. Any messages that cannot be delivered will simply remain in the gateway's mailbox until they are collected by the domain or are successfully delivered later; they will not be moved into the remote queue or retry system.

Apply this MBF File to Incoming Messages

The MBF file specified here will be applied to all incoming messages that arrive for the domain. This allows for any special reformatting that may be required.

ESMTP ETRN



ESMTP ETRN

☑ Respond to ESMTP ETRN requests made for this domain

○ Spool all mail to this host

When an ETRN request for this domain is received all stored mail should be spooled to this SMTP host.

☑ If the domain listed above is local treat it as if it were foreign.

It is sometimes desired to spool the mail to a local domain yet do so in a way that mimics remote mail processing.

● Spool all mail to IP of machine making ETRN request

Since the ETRN request might be made using a dialup connection MDaemon should respond by spooling mail to the IP address of the machine making the ETRN request.

Use this port when spooling mail: 25

IP Access

● Honor ETRN/ATRN requests from these IP's

○ Ignore ETRN/ATRN requests from these IP's

Add new IP - Wildcards (192.168.0.*) ok.

..*.*

ESMTP ETRN

Respond to ESMTP ETRN requests made for this domain

When this switch is enabled MDaemon will respond to ESMTP ETRN requests made by qualified hosts on behalf of the domain for which MDaemon is acting as an email gateway. The ETRN command is an SMTP extension that signals a server storing mail for a particular domain that it is time to begin spooling the mail. When MDaemon receives an ETRN request for a domain, it will immediately begin spooling the stored mail for delivery using subsequent SMTP transactions. Please note that the SMTP session that issues an ETRN request will not be the one that receives any stored mail. MDaemon will use subsequent independent SMTP transactions to send any mail it has stored for the domain. This preserves the message envelope and is more secure. Also note that the host to which MDaemon will spool any stored mail may not immediately begin reception of these messages. ETRN only guarantees that any stored mail is *spooled* for delivery. The actual *process* of delivery is subject to other administrator-imposed restrictions and may have to wait in the outbound mail queue for the next scheduled remote mail processing event to take place. Because of these limitations we recommend using On-Demand Mail Relay (ODMR) and its ATRN command rather than ETRN. This method is not supported by all clients and servers, however, and will therefore only be available to client domains using a server that does so. MDaemon fully supports ODMR on both the client and server side.

Spool all mail to this host

This is the host name or IP address to which any stored mail will be sent when an ETRN request is received and honored. This machine must be running an SMTP server to receive these messages.

If the domain listed above is local treat it as if it were foreign

Activate this control if the domain is local but you want its mail to be spooled as if it is remote.

Spool all mail to IP of machine making ETRN request

Selecting this option will cause MDaemon to send any stored mail to the IP address of the machine that made the ETRN request. The requesting machine must be running an SMTP server to receive these messages.

Use this port when spooling mail

Use this control to specify the port on which the domain's mail will be spooled.

IP Access

Honor ETRN/ATRN requests from these IPs

Select this switch and MDaemon will honor ETRN/ATRN requests made from any IP listed in the associated address list.

Ignore ETRN/ATRN requests from these IPs

Select this switch and MDaemon will ignore ETRN/ATRN requests that are made from any IP listed in the associated address list.

Add new IP

To add a New IP to the current list simply enter the IP into this text box and click the ADD button.

Remove

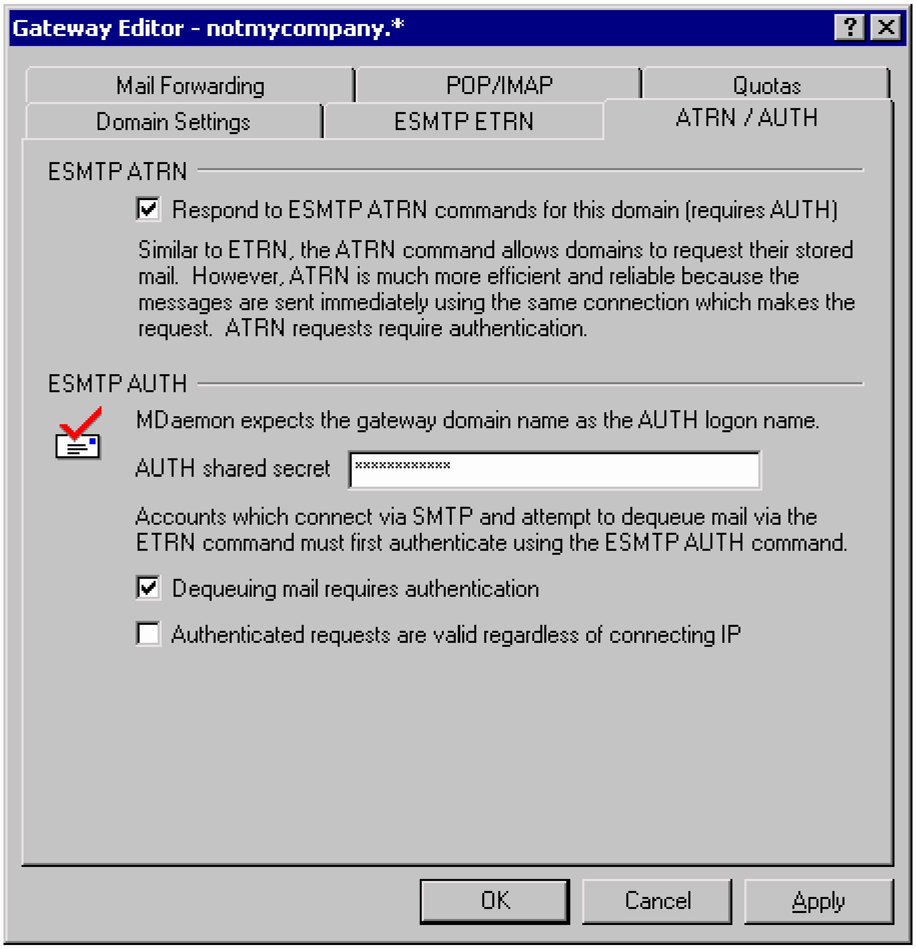
Click this button to remove a selected entry from the list of IP addresses.

Tip

Although there is nowhere on this screen to enter it, you can control the SMTP envelope ID that MDaemon will use when spooling the domain's mail. The following key controls this in the GATEWAYS.DAT file:

```
[GatewayDomainName]
EtrnAs=address@domain.com
```

ATRN / AUTH



ESMTP ATRN

☑ Respond to ESMTP ATRN commands for this domain (requires AUTH)

Similar to ETRN, the ATRN command allows domains to request their stored mail. However, ATRN is much more efficient and reliable because the messages are sent immediately using the same connection which makes the request. ATRN requests require authentication.

ESMTP AUTH

MDaemon expects the gateway domain name as the AUTH logon name.

AUTH shared secret: *************

Accounts which connect via SMTP and attempt to dequeue mail via the ETRN command must first authenticate using the ESMTP AUTH command.

☑ Dequeuing mail requires authentication

□ Authenticated requests are valid regardless of connecting IP

ESMTP ATRN

Respond to ESMTP ATRN commands for this domain (requires AUTH)

Activate this control if you want MDaemon to respond to ATRN commands from the domain for which MDaemon is acting as a gateway. ATRN is a new ESMTP command used in On-Demand Mail Relay (ODMR), which is currently the best relay method available for mail hosting. It is superior to ETRN and other methods in that in requires authentication before mail is dequeued and does not require a static IP address. A static IP address isn't required because the flow of data between MDaemon and the client domain is immediately reversed and the messages are despooled without having to make a new connection—unlike ETRN, which uses a separate connection after the ETRN command is sent. This enables client domains using a dynamic (non-static) dialup account to collect their messages without having to use POP or DomainPOP to distribute them to their users because the original SMTP envelope is preserved.

ESMTP AUTH

AUTH shared secret

Enter the client domain's "Shared Secret" or password here that will be used during authentication.

Note

The domain for which MDaemon is acting as a gateway must use its domain name as the logon parameter.

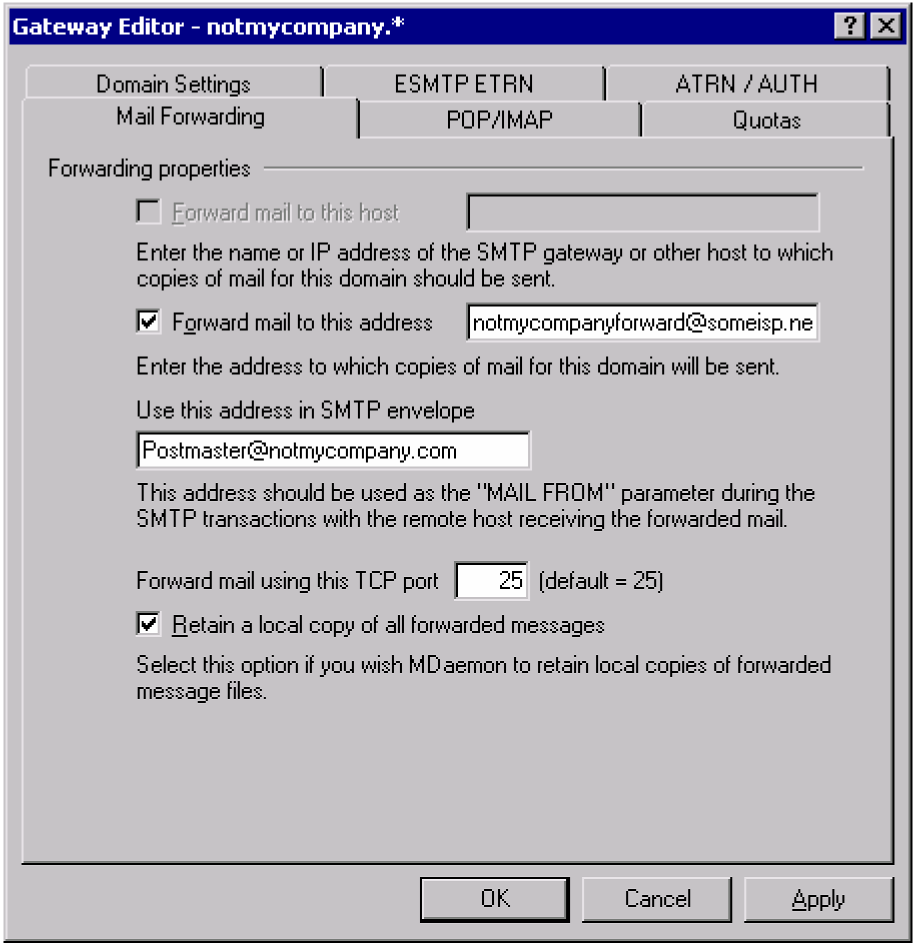
Dequeuing mail requires authentication

When you have configured the settings for this domain to accept ESMTP ETRN requests, you may use this tab's controls to require the connecting host to first authenticate itself using the ESMTP AUTH command. Since ATRN requires authentication, this control must be enabled before MDaemon will respond to ATRN requests.

Authenticated requests are valid regardless of connecting IP

Enable this checkbox if you want to honor authenticated requests regardless of the IP address from which they are coming. If this control is not enabled then only requests from those IP addresses specified in the IP Access section of the ESMTP ETRN tab (page 292) will be honored.

Mail Forwarding



Gateway Editor - notmycompany.*

Forwarding properties

□ Forward mail to this host

Enter the name or IP address of the SMTP gateway or other host to which copies of mail for this domain should be sent.

☑ Forward mail to this address: notmycompanyforward@someisp.ne

Enter the address to which copies of mail for this domain will be sent.

Use this address in SMTP envelope: Postmaster@notmycompany.com

This address should be used as the "MAIL FROM" parameter during the SMTP transactions with the remote host receiving the forwarded mail.

Forward mail using this TCP port: 25 (default = 25)

☑ Retain a local copy of all forwarded messages

Select this option if you wish MDaemon to retain local copies of forwarded message files.

Forwarding Properties

Forward mail to this host
Sometimes it is advantageous to simply forward a copy of all messages for a domain as they arrive. If you wish to configure MDaemon to do this then enter the name or IP address of the SMTP server to which copies of incoming mail for this domain should be sent.

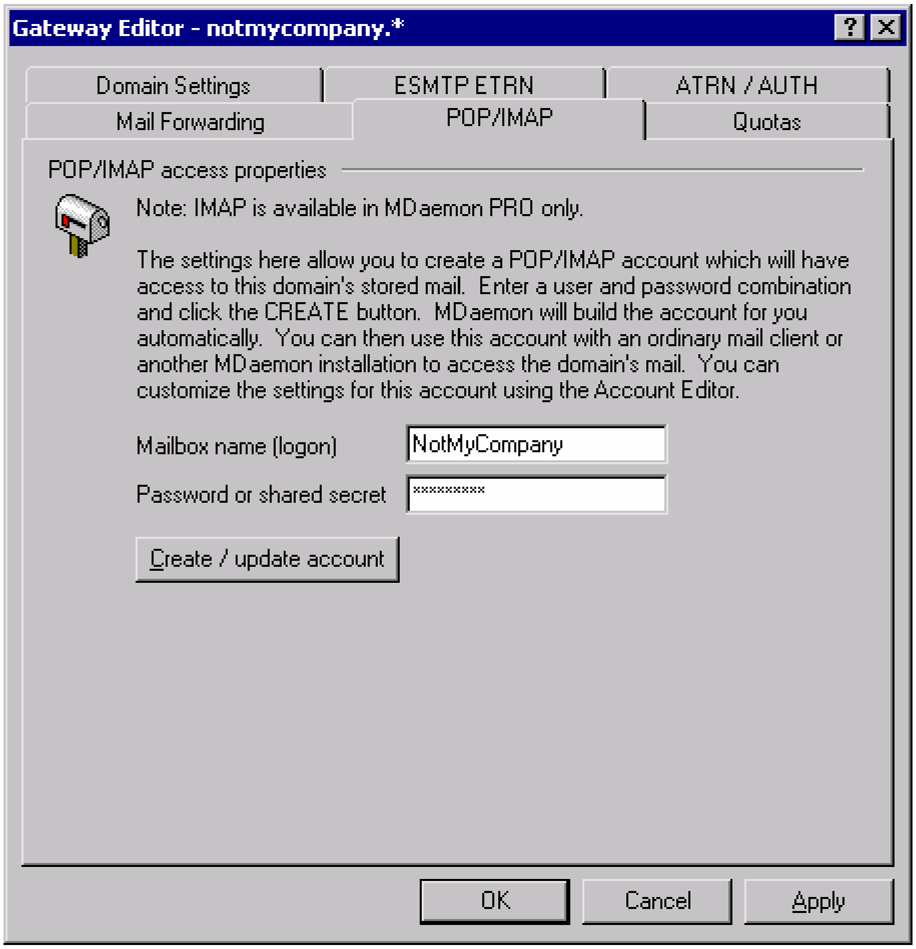
Forward mail to this address
Use this feature if you wish to forward to a specific email address all email messages destined for this client domain.

Use this address in SMTP envelope
MDaemon will use this address in the SMTP “Mail From” transaction.

Forward mail using this TCP port
MDaemon will forward this mail using this TCP port.

Retain a local copy of all forwarded messages
Select this option if you wish MDaemon to retain a copy of a message locally once it has been forwarded.

POP/IMAP



Gateway Editor - notmycompany.*

POP/IMAP access properties

Note: IMAP is available in MDaemon PRO only.

The settings here allow you to create a POP/IMAP account which will have access to this domain's stored mail. Enter a user and password combination and click the CREATE button. MDaemon will build the account for you automatically. You can then use this account with an ordinary mail client or another MDaemon installation to access the domain's mail. You can customize the settings for this account using the Account Editor.

Mailbox name (logon) NotMyCompany

Password or shared secret **********

Early versions of MDaemon pioneered a method of mail collection known as DomainPOP (see page 152). Besides using MDaemon to collect mail via DomainPOP it can also be used to act as a DomainPOP host for other domains for which your MDaemon is acting as an email gateway. In other words, all messages for the domain can be collected in a single mailbox on your server. Then, the domain can connect to you and collect them by using their own MDaemon, or by using a regular POP client instead of an MDaemon, athough in that case DomainPOP parsing would not be available to them. The controls on this dialog are used to create the account that MDaemon will use for storing the Domain Gateway's mail.

Because MDaemon Pro supports the IMAP email protocol, accounts created in MDaemon Pro can also be accessed by clients using that protocol instead of just the POP protocol.

Mailbox Name (logon)
Enter the POP USER name that the client domain will use to access the messages stored in its mailbox.

Password or shared secret
Enter the password or shared secret that the client's domain will use to access the messages stored in its mailbox.

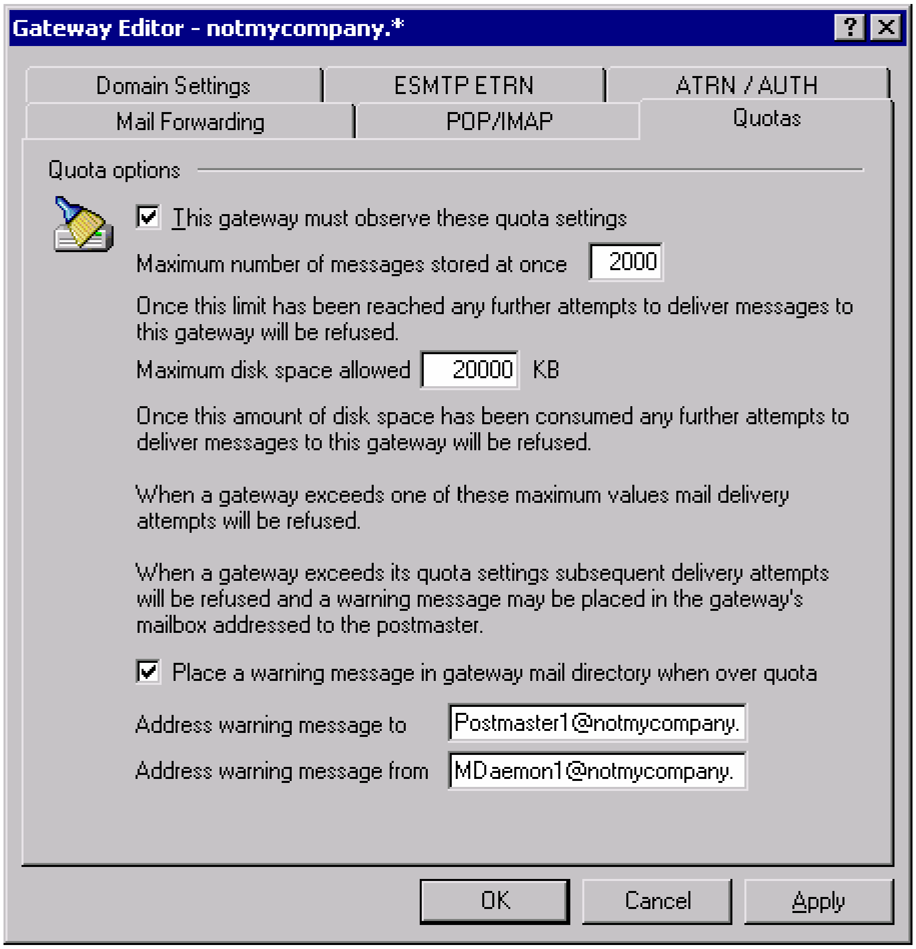
Create/update account

Click here to create an account or to update the Mailbox name and Password values if the account already exists.

Note

You can completely edit (or even remove) an account using the Account Editor. Be careful if you remove an account because that will delete the account's mail and file directories - which also happen to be the ones the gateway is using.

Quotas



Quota options

☑ This gateway must observe these quota settings

Maximum number of messages stored at once: 2000

Once this limit has been reached any further attempts to deliver messages to this gateway will be refused.

Maximum disk space allowed: 20000 KB

Once this amount of disk space has been consumed any further attempts to deliver messages to this gateway will be refused.

When a gateway exceeds one of these maximum values mail delivery attempts will be refused.

When a gateway exceeds its quota settings subsequent delivery attempts will be refused and a warning message may be placed in the gateway's mailbox addressed to the postmaster.

☑ Place a warning message in gateway mail directory when over quota

Address warning message to: Postmaster1@notmycompany.

Address warning message from: MDaemon1@notmycompany.

Quota Options

This gateway must observe these quota settings

Here you can specify the domain’s maximum number of allowable messages and the maximum amount of disk space (in kilobytes) that it can consume. This includes any decoded file attachments in its Files directory.

Place a warning message in gateway mail directory when over quota

If this control is enabled and a mail delivery to the domain is attempted that would exceed the maximum message or disk space limitations, the message will be forwarded to the designated address along with an appropriate warning.

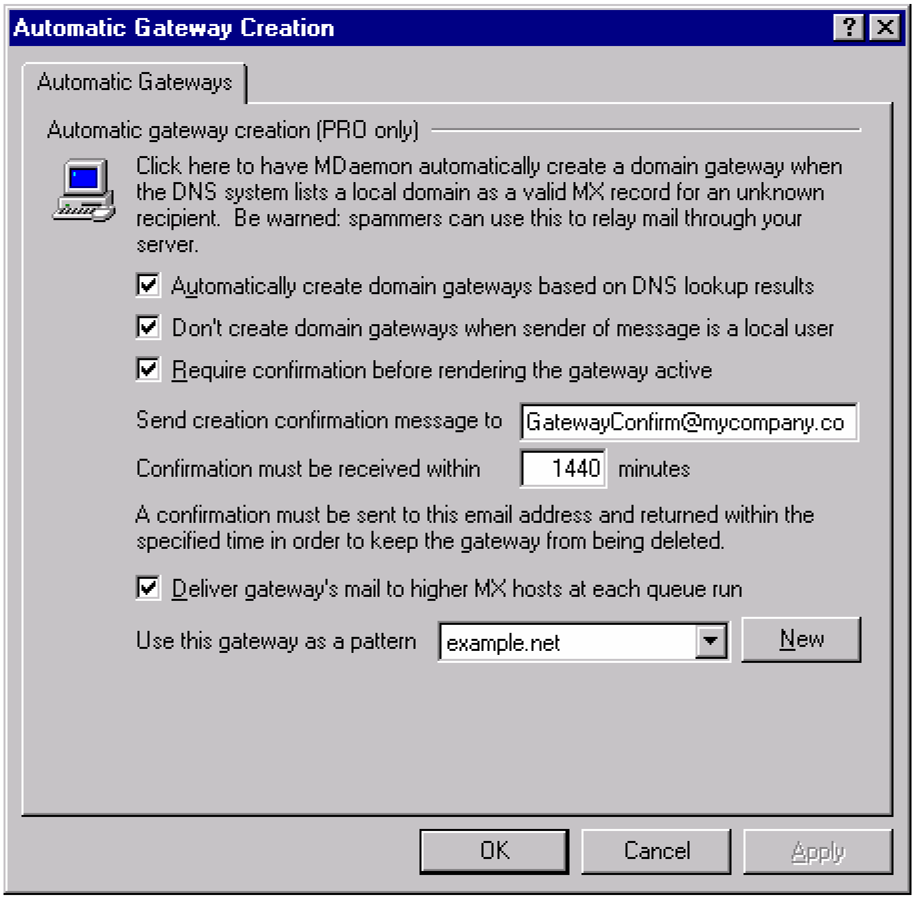
Address warning message to

Specify the address to whom the over quota warning message should be sent.

Address warning message from

Specify the address from whom the over quota warning message should appear to have been sent.

Automatic Gateway Creation



Automatic Gateway Creation

Automatic Gateways

Automatic gateway creation (PRO only)

Click here to have MDaemon automatically create a domain gateway when the DNS system lists a local domain as a valid MX record for an unknown recipient. Be warned: spammers can use this to relay mail through your server.

☑ Automatically create domain gateways based on DNS lookup results

☑ Don't create domain gateways when sender of message is a local user

☑ Require confirmation before rendering the gateway active

Send creation confirmation message to GatewayConfirm@mycompany.co

Confirmation must be received within 1440 minutes

A confirmation must be sent to this email address and returned within the specified time in order to keep the gateway from being deleted.

☑ Deliver gateway's mail to higher MX hosts at each queue run

Use this gateway as a pattern example.net

Automatic Gateways

The controls on this tab are used to configure MDaemon to automatically create a Domain Gateway (page 289) for a previously unknown domain when another source attempts to deliver that domain's messages to MDaemon, and a DNS query lists MDaemon's location as a valid MX record.

For example:

With automatic gateway creation enabled, if MDaemon's primary domain IP address is `1.2.3.4` and a message is delivered via SMTP for an unknown domain `example.com`, MDaemon will perform MX and A-record queries on `example.com` to see if `1.2.3.4` is a known mail relay host for it. If the results of the DNS queries state that MDaemon's IP address is a valid MX host for `example.com` then MDaemon will automatically create a new Domain Gateway for it and accept its email. Messages for `example.com` will then be stored in a special folder and, if you so choose, spooled to higher level MX hosts at each remote mail processing interval. This feature effectively enables you to become a backup server for another domain by simply configuring the DNS system to use your IP as an alternate MX host.

To help secure this feature, MDaemon can be configured to send a confirmation request to an email address of your choice. While MDaemon is waiting for the confirmation response, messages for the domain will be accepted and stored but not delivered. Confirmation requests must be replied to within an amount of time that you designate or the automatically created gateway will be removed and all stored messages deleted. If confirmation is received before the time has expired then the stored messages will be delivered normally.

> ☝ **Caution!**
>
> It might be possible for a malicious person or "spammer" to attempt to exploit this feature by configuring their DNS server to list your MDaemon's IP address as one of their MX hosts. Automatic Gateway Creation must therefore be used with caution. To aid in preventing possible exploitation we recommend utilizing the *Send creation confirmation message to…* feature whenever possible.

Automatically create domain gateways based on DNS lookup results
Click this checkbox if you want MDaemon to automatically create Domain Gateways based upon the results of DNS queries.

Don't create domain gateways when sender of message is a local user
Enable this control if you do not want messages originating from local users to trigger automatic gateway creation.

Require confirmation before rendering the gateway active
When this control is enabled, MDaemon will send a confirmation message to the email address of your choice in order to determine whether the automatically created gateway is valid. MDaemon will continue to accept messages for the domain in question but will not deliver them until confirmation is received.

Send creation confirmation message to
Use this textbox to list the address to which you wish confirmation messages to go.

Confirmation must be received within XX minutes
This control is for designating the number of minutes that MDaemon will wait for a response to any given confirmation message. If this time limit expires then the Domain Gateway in question will be deleted.

Deliver gateway's mail to higher MX hosts at each queue run
If you want MDaemon to attempt to deliver this gateway's messages to higher level MX hosts each time that the remote queue is processed then enable this control.

Use this gateway as a pattern
Choose a Domain Gateway from this drop-down list and MDaemon will use its settings as a template for all future automatically created gateways.

New
Clicking the *New* button will open the Gateway Editor, which can be used to create a new Domain Gateway.

Chapter

27

Queue and Statistics Manager

Using MDStats, MDaemon's queue and statistics manager.

MDaemon's queue and statistics manager (**MDStats**) is accessed directly from within MDaemon by choosing the **Queues|Queue and Statistics Manager…** menu selection. **MDStats** is made up of a four-page dialog. Each of these pages has been designed to serve a distinct and specific purpose while also maintaining a simple format that makes them very easy to use.

Queue Page

The default tab is the *Queue Page*. From this page you can easily manage all of MDaemon's standard mail queues, as well as the User Account mailbox folders. By simply clicking on the queue or user of your choice, a list of all message files contained within the specified queue will be displayed along with several key pieces of pertinent information about each message: the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location. In addition, controls are provided that make it easy to copy or move messages between folders, or delete them completely.

User Page

The *User Page* displays a list of all MDaemon users. This list includes their full name, mailbox name, the number of messages in their mailbox, the amount of disk space that their account is taking up, and the date that they last checked their mail. This list can also be saved to disk as a text file, or it can be saved in comma delimited format for use with databases.

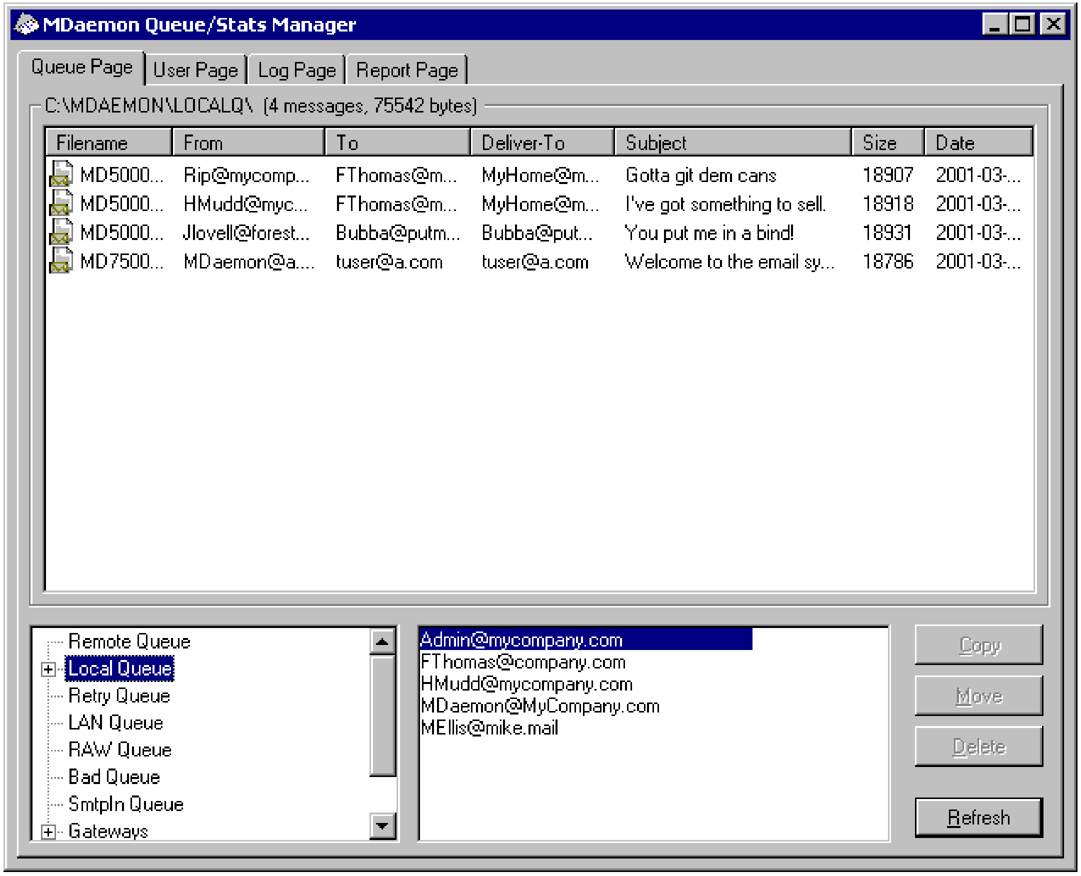
Log Page

With this dialog you can display MDaemon's *Log Files* in a simple list format. This feature is very useful for quickly examining the history of MDaemon's mail transactions because it condenses the selected *Log File* into a columnar list which contains: the Type of the message (POP Inbound, DomainPOP, RFC822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful. You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Logs displayed on the *Log Page* can be saved as a text file or in comma delimited format for use with databases.

Report Page

The last tab is the *Report Page.* With this feature you can produce a report containing all of MDaemon's configuration settings, written in a plain text readable format. Because of the large number of optional settings and configurations in MDaemon, this can greatly speed the process of administering configuration changes as well as aid in diagnosing possible configuration problems. Additionally, this report is displayed in a text editable format that makes it possible to Copy/Paste the information it contains (using the right-click shortcut menu), or add notations or other information to the file before saving it.

Queue Page



C:\MDAEMON\LOCALQ\ (4 messages, 75542 bytes)

Filename	From	To	Deliver-To	Subject	Size	Date
MD5000...	Rip@mycomp...	FThomas@m...	MyHome@m...	Gotta git dem cans	18907	2001-03-...
MD5000...	HMudd@myc...	FThomas@m...	MyHome@m...	I've got something to sell.	18918	2001-03-...
MD5000...	Jlovell@forest...	Bubba@putm...	Bubba@put...	You put me in a bind!	18931	2001-03-...
MD7500...	MDaemon@a....	tuser@a.com	tuser@a.com	Welcome to the email sy...	18786	2001-03-...

Admin@mycompany.com
FThomas@company.com
HMudd@mycompany.com
MDaemon@MyCompany.com
MEllis@mike.mail

Queue Page list box

When a queue or user is chosen from the *Message Queues* area or the user list box beside it, a list of all message files contained within the selected queue will be displayed in the main list box on this page. This list contains each message's file name, the sender, the recipient, the content of the "Deliver-To" header, the subject of the message, its size, and how long it has been at its current location (listed by date and time).

Above this box the complete file path to the currently displayed directory is given, as well as the number of messages displayed and the size of the directory.

You may copy, move, or delete one or more files by selecting them from the list and then clicking the appropriate button below it.

The content of these files may also be edited directly from the *Queue Page* list box. Simply double-click the file that you wish to edit (or choose "Edit" from the right-click shortcut menu) and MDStats will open the file for editing in Window's Notepad.

Note

If you want MDStats to open an editor other than Notepad by default, then you must edit the "mdstats.ini" file located in the \mdaemon\app\ directory. Change the "Editor=" key located under the [QueueOptions] section heading to "editor=youreditor.exe" (without the quotes). If the file path of the *.exe file is not in your current path, then you will have to include the path here as part of the file name.

The list box can be navigated by using the vertical or horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *Queue Page* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z, 1-2), or click twice to sort it in descending order (Z-A, 2-1). Columns can also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

Selecting Files

To select files individually Click the desired file.

To select contiguous files Click the first file in the contiguous list of files that you wish to select, then while holding down the SHIFT key, click the last contiguous file in the desired list.

Alternatively, you may use the ARROW, HOME, END, PAGE UP, and PAGE DOWN keys, while holding down the SHIFT key, to select files in contiguous order.

To select non-contiguous files Click on the desired files in the *File Name* column while holding down the CTRL key.

Message queues

Click an entry in the lower left pane and a list of all files contained within the specified queue will be displayed in the *Queue Page* list box. If you click the *User Folders* option, a list of all MDaemon users will be displayed in the *User List Box* to the right of the *Message Queues* section.

Users list box

This box displays a list of all MDaemon users when the *User Folders* option is clicked in the *Message Queues* section (lower left pane). Click a user's name to display a list of all message files currently contained in the user's mailbox folder.

Refresh

Because mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them - you should regularly click this button to refresh any list of files that you may have displayed.

Note

You can edit the MDstats.ini file to cause displayed lists to automatically refresh. To do this simply open the MDstats.ini file located in MDaemon's `\app\` directory and edit the AutoRefresh key under the [QueueOptions] heading to reflect the number of seconds that you wish to elapse between refreshes. Entering the value 0 means that you do not want the list to automatically refresh. Example: `AutoRefresh=15` (the list would refresh every 15 seconds).

Copy

When one or more files are selected, click this button to copy the selected files to another queue or user's mailbox folder. After clicking this button the *Copy Message(s)* dialog box will open, from which you can select the desired location to which you wish to copy the selected files.

Move

When one or more files are selected, click this button to move the selected files to another queue or user's mailbox folder. After clicking this button the *Move Message(s)* dialog box will open, from which you can select the desired location to which you wish to move the selected files.

Note

Files copied or moved to other queues will rarely retain their original file names. To avoid overwriting files of the same name that may already be in the queue, MDaemon always calculates the next destination filename based on the HIWATER.MRK file located in the destination folder.

Delete

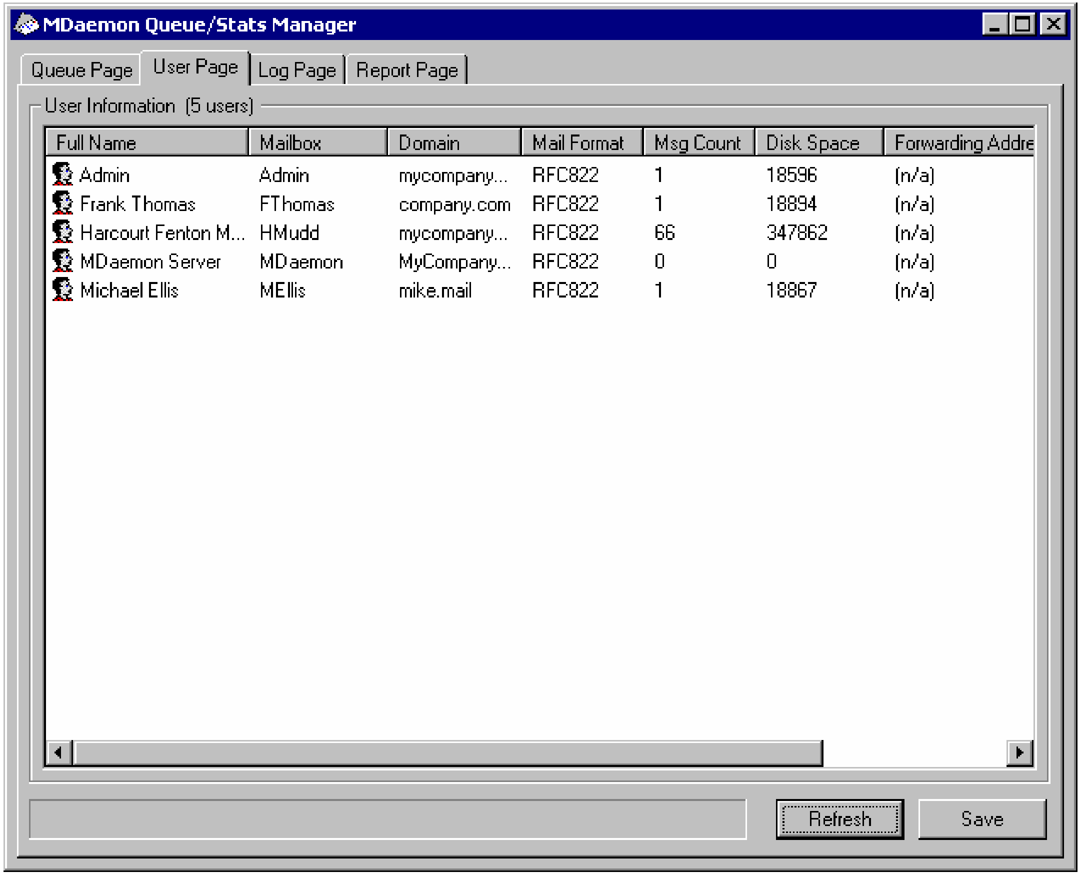
When one or more files are selected in the *Queue Status List Box*, click this button to delete the selected files. After clicking this button a confirmation box will open asking if you really do wish to delete the selected files.

Note

Mail queues are dynamic while MDaemon is active - with message files constantly being transferred to and from them. For this reason you should be aware that when copying, moving, or deleting files you may at times encounter a message from MDStats stating that it cannot complete the action that you are attempting. This will occur when the message file that you are attempting to work with has already been removed by MDaemon before the desired action has begun. By clicking the *Refresh* button, you can update the current list of files displayed in the list box.

You can prevent messages from being moved out of the queue while you are editing them by editing the MDstats.ini file. To do this simply open the MDstats.ini file located in MDaemon's \app\ directory and change the LockOnEdit=No key under the [QueueOptions] heading to LockOnEdit=Yes. This will cause a LCK file to be created whenever you are editing a message, which will prevent it from being moved out of the queue until you are finished with it.

User Page



Full Name	Mailbox	Domain	Mail Format	Msg Count	Disk Space	Forwarding Addre
Admin	Admin	mycompany...	RFC822	1	18596	(n/a)
Frank Thomas	FThomas	company.com	RFC822	1	18894	(n/a)
Harcourt Fenton M...	HMudd	mycompany...	RFC822	66	347862	(n/a)
MDaemon Server	MDaemon	MyCompany...	RFC822	0	0	(n/a)
Michael Ellis	MEllis	mike.mail	RFC822	1	18867	(n/a)

User information

When the *User Page* is chosen MDStats immediately loads a list of all MDaemon accounts into the *User Information* list box. This list contains each user's full name, the name of their mailbox, the domain to which the account belongs, the number of messages it contains, its mail format, the amount of disk space (in bytes) that the account is taking up, their forwarding address, and finally, the date that their mail was last checked. Given that the information contained in this list is constantly changing, it can be easily updated by clicking the *Refresh* button.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can sort information contained in the *User Information* list box by whichever column you choose. Simply click once on the desired column to sort it in ascending order (A-Z), or click twice to sort it in descending order (Z-A). Columns may also be resized by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width. Further, you can double-click any entry and MDStats will be shifted to the *Queue Page* with the contents of their mailbox folder displayed.

Note

By default, the list displays the Message Count not file count, and the Disk Space used *by messages* not the space used by all files in the directory. This is the *Quota* information reported by MDaemon. Alternatively, MDStats can display the *file* count and disk space used by all *files* instead of by messages. To change this setting simply open the MDstats.ini file located in MDaemon's \app\ directory and change the ShowQuota=Yes key under the [UserOptions] heading to ShowQuota=No.

Warning!

User folders contain a file called "**hiwater.mrk**" that **MDStats** reads to determine some of this user information. You should avoid deleting this file unnecessarily as it will prevent **MDStats** from being able to obtain some of the information listed in the *User Information* list box.

Refresh

User statistics such as the number of messages contained in their mailboxes, and the amount of disk space that their accounts are using, are constantly changing. You can easily update the information contained in the *User Information* list box by clicking the *Refresh* button. This will immediately make all displayed information current.

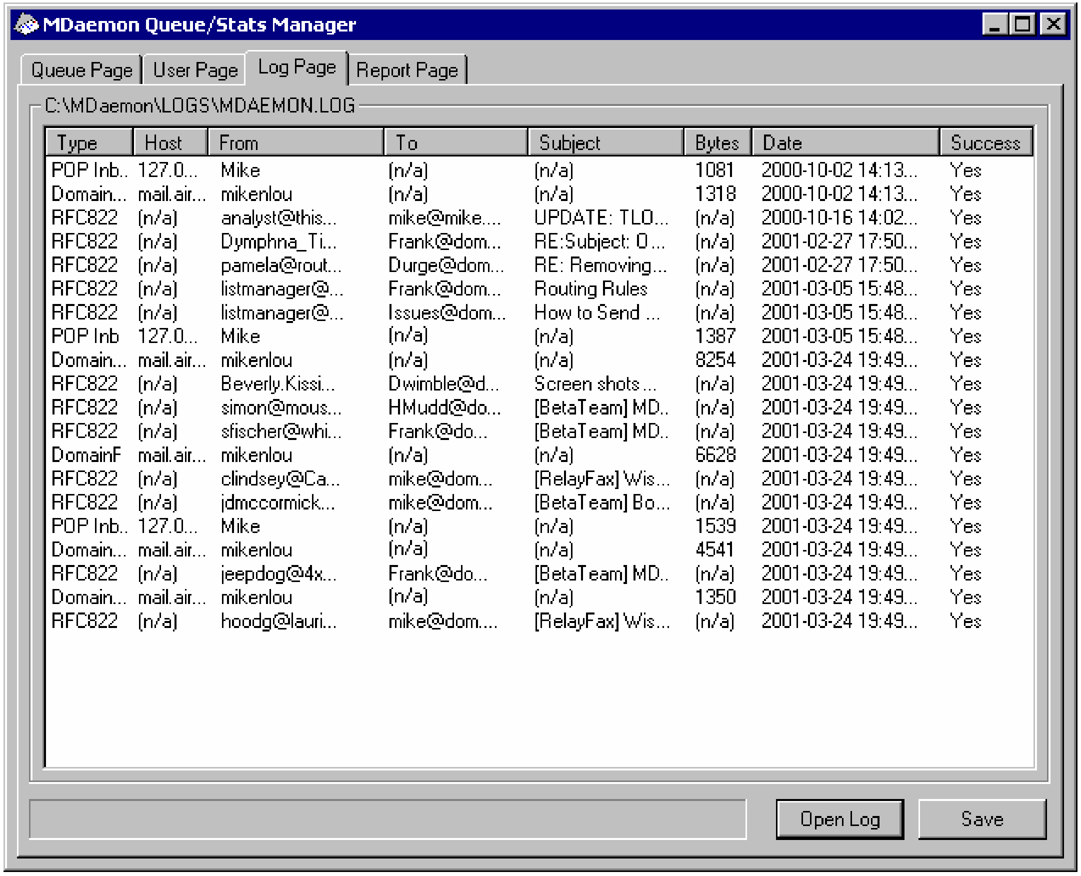
Progress indicator

Because *User Information* lists can at times be very large, below the *User Information* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded by MDStats.

Save

The information contained in the *User Information* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, MDStats will ask you whether you want to save the file in comma delimited format or as a plain text file.

Log Page



C:\MDaemon\LOGS\MDAEMON.LOG

Type	Host	From	To	Subject	Bytes	Date	Success
POP Inb..	127.0...	Mike	(n/a)	(n/a)	1081	2000-10-02 14:13...	Yes
Domain...	mail.air...	mikenlou	(n/a)	(n/a)	1318	2000-10-02 14:13...	Yes
RFC822	(n/a)	analyst@this...	mike@mike....	UPDATE: TLO...	(n/a)	2000-10-16 14:02...	Yes
RFC822	(n/a)	Dymphna_Ti...	Frank@dom...	RE:Subject: O...	(n/a)	2001-02-27 17:50...	Yes
RFC822	(n/a)	pamela@rout...	Durge@dom...	RE: Removing...	(n/a)	2001-02-27 17:50...	Yes
RFC822	(n/a)	listmanager@...	Frank@dom...	Routing Rules	(n/a)	2001-03-05 15:48...	Yes
RFC822	(n/a)	listmanager@...	Issues@dom...	How to Send ...	(n/a)	2001-03-05 15:48...	Yes
POP Inb	127.0...	Mike	(n/a)	(n/a)	1387	2001-03-05 15:48...	Yes
Domain...	mail.air...	mikenlou	(n/a)	(n/a)	8254	2001-03-24 19:49...	Yes
RFC822	(n/a)	Beverly.Kissi...	Dwimble@d...	Screen shots ...	(n/a)	2001-03-24 19:49...	Yes
RFC822	(n/a)	simon@mous...	HMudd@do...	[BetaTeam] MD..	(n/a)	2001-03-24 19:49...	Yes
RFC822	(n/a)	sfischer@whi...	Frank@do...	[BetaTeam] MD..	(n/a)	2001-03-24 19:49...	Yes
DomainF	mail.air...	mikenlou	(n/a)	(n/a)	6628	2001-03-24 19:49...	Yes
RFC822	(n/a)	clindsey@Ca...	mike@dom...	[RelayFax] Wis...	(n/a)	2001-03-24 19:49...	Yes
RFC822	(n/a)	jdmccormick...	mike@dom...	[BetaTeam] Bo...	(n/a)	2001-03-24 19:49...	Yes
POP Inb..	127.0...	Mike	(n/a)	(n/a)	1539	2001-03-24 19:49...	Yes
Domain...	mail.air...	mikenlou	(n/a)	(n/a)	4541	2001-03-24 19:49...	Yes
RFC822	(n/a)	jeepdog@4x...	Frank@do...	[BetaTeam] MD..	(n/a)	2001-03-24 19:49...	Yes
Domain...	mail.air...	mikenlou	(n/a)	(n/a)	1350	2001-03-24 19:49...	Yes
RFC822	(n/a)	hoodg@lauri...	mike@dom....	[RelayFax] Wis...	(n/a)	2001-03-24 19:49...	Yes

Log report

The *Log Report* list box displays MDaemon's detailed log files that you select through the *Open Log* button and the Windows Open dialog that follows it. The *Log Report* display provides a quick and easy way to review the history of mail transactions that MDaemon has processed without having to sort through the large volume of information that MDaemon log files may sometimes contain. When a *Log Report* is displayed in this list box MDStats breaks it down into a simple format containing: the Type of the message (POP Inbound, DomainPOP, RFC822, and so on), the Host to which MDaemon connected during the transaction, the sender, the recipient, the message size, the date that each message was processed, and whether or not the transaction was successful.

You can also examine the detailed portion of the log regarding any of the entries on the list by double clicking the desired entry. This will display the portion of the log where that transaction was made. Using the right-click shortcut menu you can copy/paste this detailed log portion to a text editor for saving or editing should you desire to do so.

The list box can be navigated by using the vertical and horizontal scroll bars, or you can click anywhere within the list box and use the ARROW keys for navigation. You can resize the list box's columns by positioning the pointer over the line between any of the column headings until it changes shape and then dragging the column to the desired width.

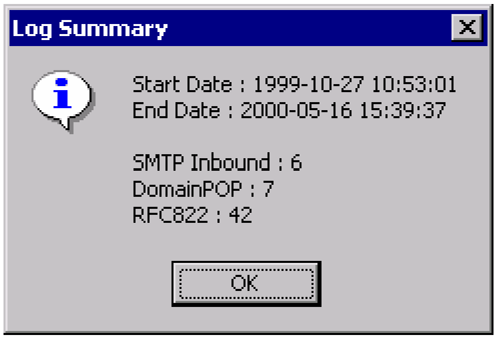
Note

The *Log Page* will display log files that have been compiled using either the *Log Detailed Mail Sessions* or the *Log Summarized Mail Sessions* option located in MDaemon's **Setup | Log File** menu selection. However, we highly recommend that you use the *Log Detailed Mail Sessions* option instead of the *Summarized* option. When using the *Log Summarized Mail Sessions* format you will find that there is very little information that will be displayed in your *Log Report*. Because the *Log Page* itself condenses the detailed log into a summary view of MDaemon's activity, while still providing the ability to look at the detailed view of every transaction when necessary (by double-clicking an entry), there is no need to have MDaemon summarize the log file while compiling it.

Open log

Click this button to open the Windows Open dialog for choosing which log file that you wish to view. The default folder that this dialog will display is the *Log File* directory that you have designated in the MDaemon menu selection **Setup | Primary Domain | Directories**. If you click this button when there is a *Log File* already displayed in the *Log Report* list box, MDStats will give you the option to append the new file to the one that is currently being displayed.

After a log is displayed, a message box will be opened which contains a summary of the selected log. When saving a Log Report as a text file, this log summary will be appended to the file being saved.



Start Date : 1999-10-27 10:53:01
End Date : 2000-05-16 15:39:37

SMTP Inbound : 6
DomainPOP : 7
RFC822 : 42

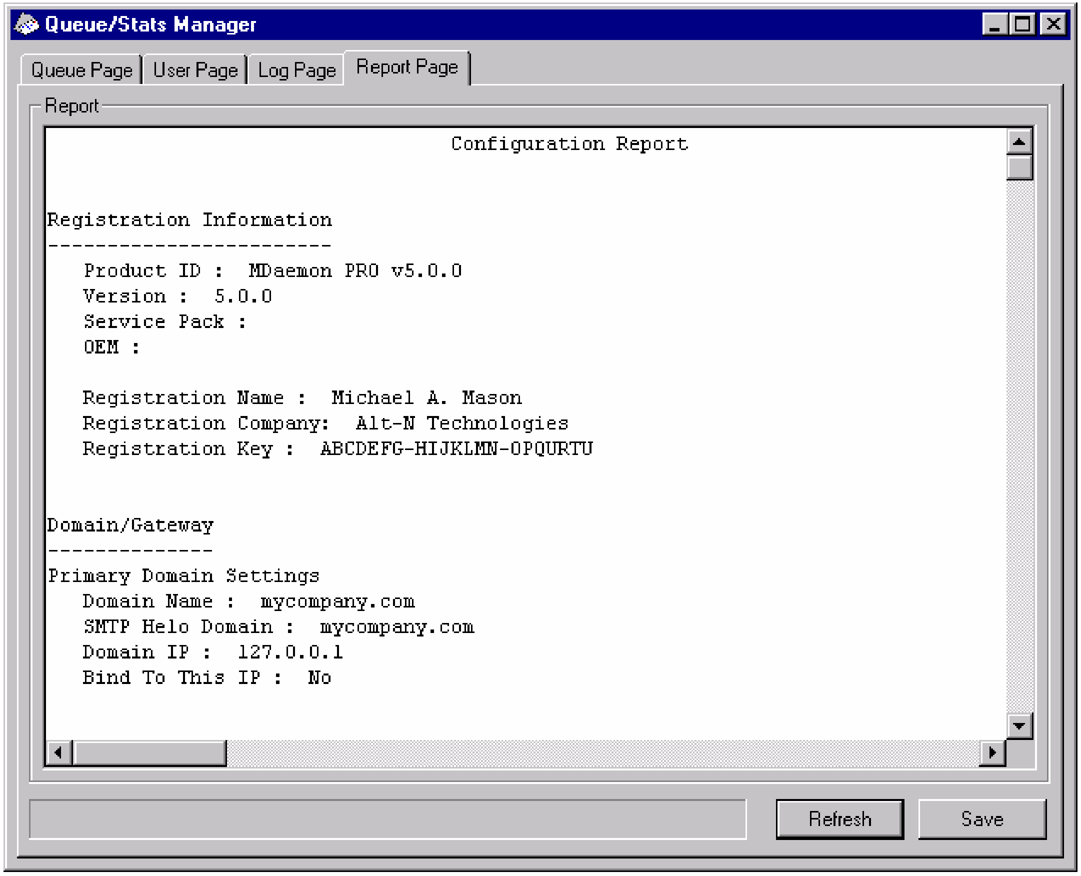
Progress indicator

Because *Log Files* can be very large, below the *Log Report* list box is a progress indicator bar that provides a visible indication that the program is still operating when large files are being loaded or saved by MDStats.

Save

The information contained in the *Log Report* list box can be saved as a file in comma delimited format for use with databases, or as a plain ASCII text file by clicking the *Save* button. After choosing a name and location for this file in the Windows Save As dialog, MDStats will ask you whether you want to save the file in comma delimited format or as a plain text file.

Report Page



```
                         Configuration Report


Registration Information
------------------------
   Product ID :  MDaemon PRO v5.0.0
   Version :  5.0.0
   Service Pack :
   OEM :

   Registration Name :  Michael A. Mason
   Registration Company:  Alt-N Technologies
   Registration Key :  ABCDEFG-HIJKLMN-OPQURTU


Domain/Gateway
--------------
Primary Domain Settings
   Domain Name :  mycompany.com
   SMTP Helo Domain :  mycompany.com
   Domain IP :  127.0.0.1
   Bind To This IP :  No
```

Report

When the *Report Page* is clicked MDStats will produce a comprehensive report that lists every setting within MDaemon in an easily readable text format. This feature greatly decreases the amount of time needed by an administrator to check MDaemon's many configuration settings, and it can aid in quickly solving possible configuration problems.

You can navigate through this report using either the scroll bars or the CURSOR keys, and the *Report* display is also a text editor - making it possible to insert notations or additional information that you may want on the report before saving it to a file. Additionally, you can use the shortcut menu to Cut, Copy, and Paste, to and from this display by right-clicking your mouse and making the desired selection from the menu that opens.

Refresh

Click this button to update the currently displayed *Report* of MDaemon settings.

Progress indicator

As with the other tabs in MDStats, the *Report Page* contains a progress indicator bar that serves as a visible indicator that the program is still operating while large files are being loaded or saved.

Save

Click this button to save the currently displayed *Report*. After clicking this button a standard Save As dialog will open so that you can designate a file name and location where you want to save it.

Customizing the Queue/Statistic Manager

The following is a list of settings that can be modified in the MDstats.ini file located in MDaemon's \app\ directory:

MDstats.ini File

[MDaemon]	
AppDir=C:\mdaemon\app\	Location of MDaemon's \app\ directory.
[QueueOptions]	
Editor=NOTEPAD.EXE	Editor to use when a message is double-clicked, or when a message is right-clicked and then Edit is selected.
LockOnEdit=No	Whether or not to create a LCK file when editing a message. This will prevent a message from being moved out of the queue while it is being edited.
AutoRefresh=Yes	Time (in seconds) between auto refreshes of the message listing. 0 means no auto refresh.
ShowDirectories=Yes	Show subdirectories of the queues in the list box in addition to the messages. Directories will appear as <DirectoryName>.
[UserOptions]	
ShowQuota=Yes	Determines whether the user listing displays quota information (message count and disk space just like MDaemon calculates it) or file information (number of files and total disk space).
[LogOptions]	
ShowUnknown=Yes	Show sessions that MDStats couldn't determine if they were inbound or outbound, SMTP or POP.
ShowSmtpInbound=Yes	Show SMTP inbound sessions.
ShowPopInbound=Yes	Show POP inbound sessions (mail checks).
ShowSmtpOutbound=Yes	Show SMTP outbound sessions.
ShowPopOutbound=Yes	Show POP outbound sessions (MultiPOP, DomainPOP).
ShowRFC822=Yes	Show RFC822 local mail deliveries.
ShowSmtpHelo=Yes	For SMTP inbound sessions, show HELO domain in the Host column.
IgnoreEmptyPop=Yes	Ignore mail checks when no mail was deliverd.

ShowImap=Yes	Shows IMAP Sessions.
[Remap]	Drive letter remapping; for running MDStats from a different machine than the one MDaemon is on.
C:=\\server\c	When reading from MDaemon.ini, replace "C:" with "\\server\c".
[Special]	
OnlyOneInstance=No	Allow only one instance of MDStats to run. Attempting to open it again will activate the instance that is already running. This option can be set on the GUI tab of Miscellaneous Options by enabling or disabling the control: "Restrict MDStats GUI to a single instance only".

MDStats Command Line Parameters

Note: All command line parameters are not case sensitive.

Number 1 through 8	Display a specified queue in the Queue Page.
	1 = Remote Queue
	2 = Local Queue
	3 = Retry Queue
	4 = LAN Queue
	5 = RAW Queue
	6 = Bad Queue
	7 = SmtpIn Queue
	8 = Save Queue
/L[N] [InputFile] [OutputFile]	Produce a log file report. Specifying an 'N' after the 'L' means do not save as a comma delimited file.
/A	If producing a log file report, append new information to the output file rather than overwriting it.

Chapter

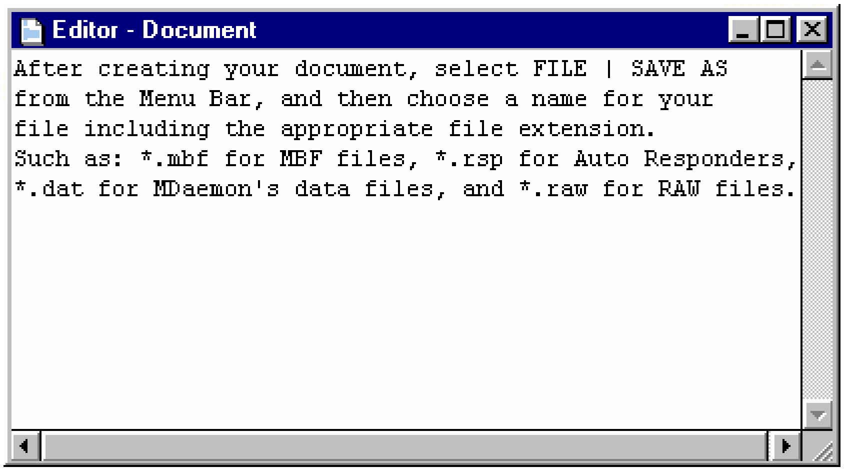
28

Additional MDaemon Features

Additional Features, Functions, and Statistics of MDaemon v6.

MDaemon's Text Editor

MDaemon Server v6 provides a **Text Editor** which may be opened with the **FILE | NEW** menu selection. The Text Editor can be useful for quickly creating *data* files for use with **Auto Responders** and various other MDaemon features, such as **MBF** and **RAW** files.



```
After creating your document, select FILE | SAVE AS
from the Menu Bar, and then choose a name for your
file including the appropriate file extension.
Such as: *.mbf for MBF files, *.rsp for Auto Responders,
*.dat for MDaemon's data files, and *.raw for RAW files.
```

Editing MDaemon Files

MDaemon's text editor can also be used to edit a number of existing files used by MDaemon. You can open these files by using the menu option: **File|Open|[Filename]**. If the file that you wish to edit is not listed on the **Open** menu then click the **Generic Document** option. When you have finished editing the file click **File|Save** or **Save As…**

Here is a list of all the documents currently listed on the **Open** menu:

- Current version release notes

——

- Server usage policy statement
- HELP message

- New user welcome message
- Account information message
- Transient delivery failure message
- Permanent delivery failure message
- Delivery return-receipt message
- "No valid command found" message
- "No such user here" message

- MX cache database
- IP cache database
- IP shield database
- No-cache database
- Relay control database
- Address alias database
- Header translation database
- MIME type definition database
- IP screen database
- Priority mail database

The RAW Message Specification v3.1

MDaemon Server v6 has inherent support for a simple and powerful mail message format known as RAW mail. This specification was developed in 1994 for a corporation that needed a custom MTA focusing on easy mail client development. The purpose of the RAW system is to provide a simple and standard format which software systems such as MDaemon can use to create the much more complex RFC-822 compliant message. Use of mail transport agents such as RAW allow client software to offload to the server all the complicated work of maintaining adherence to Internet mail standards.

RAW mail consists of a series of required and optional text headers followed by a message body. Most headers consist of a token followed by a value enclosed in <> symbols. Each header line ends with a <CRLF> combination of characters. All text, headers and body, are plain ASCII and are contained in a file which ends with the extension: RAW. Headers are separated from the message body by a blank line and are case insensitive. The *from* and *to* headers are the only ones which are required.

From <mailbox@host.com>	This field contains the email address of the sender.
To <mailbox@host.com [, mailbox@host.com]>	This field contains the email address(es) of the recipient(s). Multiple recipients can be specified by separating each one with a comma character.
ReplyTo <mailbox@host.com>	An optional email address where replies to this message will be directed.
CC <maibox@host.com [, mailbox@host.com]>	An optional list of carbon copy recipients of this message. Multiple carbon recipients can be specified by separating each one with a comma character.
Subject <text>	An optional subject for the message.
Header <Header: Value>	Allows you to explicitly place Header/Value combinations into the message.

Special fields supported by RAW v3.1

File attachment and encoding:

```
X-FLAG=ATTACH <filepath, method> [-X]
```

Example: `X-FLAG=ATTACH <c:\utils\pkzip.exe, MIME> -x`

This X-FLAG specifies the value "ATTACH" along with two parameters within the <> characters. The first parameter is a complete path to the file which should be attached to the message. The second parameter which is separated from the first by a comma character and specifies the method of encoding that is to be used when attaching the message. **MDaemon Server v6** supports two values for this parameter. The method of MIME instructs the server to use the Internet standard Base64 method of message encoding. The method of ASCII instructs the server to simply import the file into the message. An optional -X parameter at the end of the string instructs the server to remove the file from disk once it has been attached.

Delivery Status Notification:

```
X-FLAG=CONFIRM_DELIVERY
```

When converting a RAW message which contains this flag into RFC-822 mail, the string is transformed to the "Return-Receipt-To: <sender@host.org>" construct.

Placing Specific Header/Value Combinations Into the RFC-822 Message:

If you wish to place a specific header/value combination into the RFC-822 message which will be generated from a RAW file, you will need to use the HEADER macro. For example, if you want the header "Delivered-By: mail-machine@domain.com" to be placed into the RFC-822 message you would place this: "header <Delivered-By: mail-machine@domain.com>" in the RAW message. Note that the "header" macro requires both the field and value. You can place as many "header" macros as you need into a RAW message.

Sample RAW mail messages:

1)

```
from <mdaemon@altn.com>
to <JohnSmith@somewhere.com>

Hello John!
```

2)

```
from <JohnSmith@nowhere.com>
to <President@Whitehouse.gov>
subject <Secret FBI Files>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\secret\files\dole.zip, MIME> -X

Here are all those files you asked for.
```

Remote Server Control Via Email

Many functions of MDaemon Server v6 can be accessed remotely using the email transport system itself. For example, users can gain access to various aspects of their accounts and change or reconfigure them by sending email messages to the server. MDaemon maintains an account for its own use in the user base. This account is reached by sending mail to the mailbox "`MDaemon@MDaemonsDomain.com`". Messages sent to the server are stored in the server's message directory just like any other user. At queue run time the server will cycle through all the mail it has received and parse each message for special instructions.

Some of these control messages require a valid account on the server, and are password protected. Users can gain access to their accounts using their account password, and the messages to the server must be directed to "MDaemon@mydomain.com". For those commands which require a valid account on the server, the **Subject** field of the message must contain the user's email address and password separated with a comma character (e.g. "Bill@mydomain.com, MyPassword"). Commands are placed within the body of the message. There can be only one command per line but multiple commands can be batched in the same message.

Account Access and Control

The following section lists the current account access and control commands available to account holders. All of these commands require a "POP Name, POP Password" construction in the subject line. Parameters contained in **[brackets]** are optional. For example: "name [address]" could be entered as "Lois" alone, or with the optional parameter added ("Lois LLane@dailyplanet.com").

COMMAND	PARMS	DESCRIPTION
ACCOUNT INFO	none	The status of the account passed in the subject line is mailed back to the originator. Ex: ACCOUNT INFO
PASSWORD	new password	The password of the account passed in the subject line will be changed to the one specified. Ex: POP PASSWORD kryptonite
MAILFORMAT	MBF file	The mailbox storage format of the account specified in subject line will be changed to the one specified. A listing of the available formats can be obtained via the MAIL FORMATS command (see General Email Controls section below). Ex: MAILBOX RFC-822
AUTODECODE	Y/N	Automatic decoding of incoming MIME attachments for the account specified in the subject line will be turned on or off. Y=on, N=off. Ex: AUTODECODE Y
BEGIN SIGNATURE	none	Begins recording of a new signature file to be appended to messages generated by the account passed in the subject line. Subsequent lines will be treated as the text of the signature file until the word END is encountered on a line by itself or the end of the control message is reached. **NOTE:** The signature file feature is only available for RAW format messages. RFC-822 mail that arrives at the server using SMTP or POP will not append the signature file. In these cases see your mail client's documentation for information concerning signature files.
BEGIN AUTORESPONDER	none	Begins recording of a new autoresponder file. Subsequent lines will be treated as the text of the autoresponder until the word END is encountered on a line by itself or the end of the control message is reached. Ex: BEGIN AUTORESPONDER I'm on vacation right now. I'll get back to you ASAP. END To erase an active autoresponder, use the same command but without any response text. Ex: BEGIN AUTORESPONDER END

FORWARD TO	address	The forwarding address for the account passed in the subject line will be changed to [address] and mail forwarding will be activated for the account. Ex: FORWARD TO vacationing@myhost.com
UNFORWARD	none	Mail forwarding will be deactivated for the account specified in the subject line. Ex: UNFORWARD
MULTIPOP	on/off	MultiPOP will be enabled/disabled for the account specified in the subject line. Ex: MULTIPOP ON Ex: MULTIPOP OFF

Mailing List and Catalog Control

None of these commands require an account on the server; thus the subject line need not contain any special value when specifying these instructions. Parameters contained in **[brackets]** are optional. For example: “name [address]” could be entered as “Clark” alone, or with the optional parameter added: “Clark CKent@dailyplanet.com”. Command parameters listed in “{ }” or “( )” require those symbols to be used.

COMMANDS	PARMS	DESCRIPTIONS
USERS	none	A listing of all user accounts which are not flagged to hide their information will be mailed back to the message originator. Ex: USERS
LIST	none	A listing of all non-concealed named lists (*Mailing Lists* that are configured to respond to LIST commands) along with the names and addresses of all members will be mailed back to the message originator. Ex: LIST
	[listname]	Retrieves the membership of the list “LISTNAME” if it is configured to respond to the LIST command. Ex: LIST MDSUPP
	[listname (listpass)]	This command retrieves the membership of the list “LISTNAME” even if it is configured to ignore the LIST command; as long as the list password is correct. Parentheses around the list password ARE required. Ex: LIST MDSUPP (THERIGHTPASSWORD)
SUBSCRIBE	listname [address] [{real name}] [(pass)]	The originator is added to the membership of the specified list provided that list exists and allows remote subscriptions. If an optional address is specified after the list name then that address is added to the list’s membership rather than the address found in the FROM: field of the subscription message. A real name can be added for the subscriber by including it in braces (e.g. {Frank Thomas}. If the list’s password follows this command (parentheses around it are required) then the command will be honored even if this list’s subscribe function is switched off. Ex: SUBSCRIBE mdsupp Ex: SUBSCRIBE mdsupp me@mydomain.com {Frank Thomas} Ex: SUBSCRIBE mdsupp you@yourdom.com (MDPASS)
UNSUBSCRIBE or SIGNOFF	listname [address] [(pass)]	The originator is removed from the membership of the specified list provided that list exists and contains the originator as a current member. If an optional address is specified after the list’s name then that address is removed from the list’s membership rather than the address found in the FROM: field of the unsubscribe message. If the list’s password follows this command (parentheses around it are required) then the command will be honored even if this list’s unsubscribe function is switched off. Ex: UNSUBSCRIBE MDSUPP (MDSPASS) Ex: SIGNOFF MDSupportList me@mydomain.com

UPDATE	listname old-address new-address {real name} (password)	Removes “old-address” from the list and replaces it with “new-address”. An optional real name and password value may be given. Ex: UPDATE mdsupp@altn.com old@my.com new@my.com {Mr. M} Ex: UPDATE mdsupp@altn.com old@my.com new@my.com (pass)
SUPPRESS	listname address (password)	This command adds 'address' to the lists suppression file. The list's password must be provided and the list must already have a suppression file associated with it. Ex: SUPPRESS list@mydomain.com Ex: SUPPRESS me@mydomain.com (PASS)
UNSUPPRESS	listname address (password)	This command removes 'address' from the lists suppression file. The list's password must be provided and the list must already have a suppression file associated with it. Ex: UNSUPPRESS list@mydomain.com Ex: UNSUPPRESS me@mydomain.com (PASS)
DIGEST	listname [address]	The sender is set to receive mail from the list in digest format. If an optional address is specified after the list name then that address is set to digest mode. Ex: DIGEST MDSupportList Ex: DIGEST mdsupp joe@mdaemon.com
NORMAL	listname [address]	The sender is set to receive mail from “list” in normal (non-digest) format. If an optional address is specifed after the list name then that address is set to receive in normal format instead of the sender. Ex: NORMAL MDSupportList@mydomain.com Ex: NORMAL mdsupp@mydomain.com joe@mdaemon.com
NOMAIL	listname [address]	This command sets 'address' to nomail mode. The account will enter a suspended state and will no longer receive list traffic. If no address is specified then the originator of the message will be used. ex: NOMAIL list@mydomain.com me@mydomain.com
MAIL	listname [address]	This command returns 'address' to normal mode from nomail mode. If no address is specified then the originator of the message will be used. Ex: MAIL list@mydomain.com Ex: MAIL list@mydomain.com me@mydomain.com
REALNAME	listname [address] {real name}	This command sets the real name value for “address” who is a member of list “listname” to the given value. The real name must be enclosed in { and } characters. Ex: REALNAME mdsupp@altn.com {Frank Thomas}
GET	catalog magic-name (password)	Retrieves a file from the specified catalog, MIME encodes it in an email message, and sends that message to the originating account or to the one specified in a RESULTS TO directive. Ex: GET utils myutil (mypass) **NOTE: The special PUBLIC catalog doesn’t require a catalog name or password in order to retrieve a file.**
DIR	catalog	Retrieves a directory of the files and magic names available through the catalog. Ex: DIR public.

General Email Controls

COMMANDS	PARMS	DESCRIPTIONS
HELP	none	A copy of the help.dat is processed and mailed back to the message originator.
RESULTS TO	address	The results of subsequent instructions are redirected to the email address specified rather than to that of the message originator. Ex: RESULTS TO someone@somewhere.com LIST MDSUPP
STATUS	none	A status report on server operations and current conditions will be mailed back to the message originator. Since the information contained in this status report is considered private the subject of the requesting message must contain the MDCONFIG Administrator level user and password such as: Administrator, Password Ex: STATUS

MAIL FORMATS	none	A listing of all the supported mailbox formats will be mailed back to the originator. Ex: MAIL FORMATS
GET ADDRESS	none	MDaemon will send a message back to the originator which will contain the current machine name and IP address assigned to MDaemon's computer. This is useful when you want to find out the IP address assigned by your ISP when using a dynamic dial-up situation. Since the information contained in this message is considered private the subject of the requesting message must contain the MDCONFIG Administrator level user and password such as: Administrator, Password Ex: GET ADDRESS

MDaemon and Proxy Servers

MDaemon Server v6 has been purposely designed to be highly versatile. Consequently, it can be configured for use with a wide variety of network configurations and various other products. MDaemon's flexibility allows it to work well with LAN proxy servers such as WinGate. To configure MDaemon to work through any proxy server, all you must do is make sure that the port settings (see **Ports**—page 41) you are using do not conflict with any that may be set in the proxy server itself. For example, SMTP email normally takes place on port 25. Since an IP address can only have a single port 25, two servers cannot both listen for SMTP email at the same time on the same machine. When attempting to integrate MDaemon with a proxy**,** it is recommended that whenever possible, you allow MDaemon as much control over mail processing and delivery as possible. To this end, SMTP and POP ports in the proxy should be disabled so that MDaemon can handle mail delivery independently.

However, should you find it necessary to channel mail through a proxy, MDaemon allows you to configure the ports which it will use to send and receive SMTP/POP/IMAP transactions. You may need to set these ports to non-standard values in order to filter your SMTP/POP/IMAP transactions through a proxy server or firewall.

For more detailed information on configuring MDaemon to work with a proxy server, please consult the resources available at the following URL:

`http://www.mdaemon.com/helpdesk/`

Miscellaneous Information

- If you send a message to "procnow@mydomain.com" **MDaemon** will generate the `PROCNOW.SEM` file. As a result of this, you can't use "procnow" as an email mailbox for one of your accounts.
- Mail to domains listed in the LAN DOMAINS tab is kept in a directory called LNDOMAIN which stems off the LOCALQ directory.
- If you send a message to "getaddress@mydomain.com" **MDaemon** will send a message back to you telling you the domain name and IP address that has been assigned to **MDaemon's** computer. This is useful if you want to know what IP address has been assigned to your computer from your ISP when you have a dynamic dial-up situation.

Appendix A

Semaphore Files

MDaemon responds to numerous semaphore files that can be used for a variety of useful purposes. Periodically MDaemon will scan the `\APP\` subdirectory for the existence of these files. If it finds one, the associated behavior is triggered and the semaphore file is removed. This provides for a simple mechanism which will allow administrators and/or developers to manipulate MDaemon without actually handling the interface. The following is a list of all the semaphores and what they do:

FILENAME	ACTION
USERLIST.SEM	Forces MDaemon to reload the `USERLIST.DAT` file and rebuild the `EVERYONE.GRP` mailing list. Use this when you make modifications to the `USERLIST.DAT` and need MDaemon to reload it.
EDITUSER.SEM	This semaphore is used to update specific records within the `USERLIST.DAT` file without a potentially time consuming complete rebuild. To update a specific record within `USERLIST.DAT` you first construct a complete replacement record according to the format specified in the Account Management Functions section of the MDaemon API (see `MD-API.html` in MDaemon's `\docs\API\` subfolder).. The new record will reflect the changes that need to be updated within `USERLIST.DAT`. How does MDaemon know which record in `USERLIST.DAT` to update? This is accomplished by prepending the new record with the original record's email address followed by a comma. The `EDITUSER.SEM` file can contain multiple records to update – each on its own line. MDaemon will process the file one line at a time. You can create `EDITUSER.LCK` to lock the file while you are updating it and MDaemon will not touch `EDITUSER.SEM` until `EDITUSER.LCK` is deleted. To see a sample `EDITUSER.SEM` file open `EDITUSER.SMP` in your APP directory with a text editor.
ADDUSER.SEM	This semaphore creates new accounts. It is used to force MDaemon to append new records to the end of the `USERLIST.DAT` file without causing a potentially time consuming complete rebuild of the user database. Each line in this file must be a complete account record of the form specified in the Account Management Functions section of the MDaemon API (see `MD-API.html` in MDaemon's `\docs\API\` subfolder). Multiple new accounts can be specified – one account record per line. MDaemon will process the file one line at a time and add each new account. You can create `ADDUSER.LCK` to lock the file while you are updating it and MDaemon will not touch `ADDUSER.SEM` until `ADDUSER.LCK` is deleted. To see a sample `ADDUSER.SEM` file open `ADDUSER.SMP` in your APP directory with a text editor.
DELUSER.SEM	You can use this semaphore file to delete one or more user accounts. Create a text file containing the addresses of each account that you want to be deleted (one address per line), name the file "`DELUSER.SEM`" and then move it to MDaemon's …`\app\ directory`. MDaemon will delete the accounts and then delete the DELUSER.SEM file.
PROCNOW.SEM	MDaemon will immediately go into mail processing mode.
PROCLOC.SEM	MDaemon will immediately go into mail processing mode and convert all RAW files, transact all local and LAN domain mail, and process any messages waiting in the MDaemon account's mailbox.
PROCREM.SEM	MDaemon will immediately go into mail processing mode and transact all remote mail.
PROCDIG.SEM	Forces *Digests* to be sent immediately.
PROCRETR.SEM	Forces the Retry Queue to be processed.
PROCBAD.SEM	Forces the Bad Message Queue to be processed.
EXITNOW.SEM	MDaemon will terminate and remove itself from memory.
SCHEDULE.SEM	Forces MDaemon to reload the `SCHEDULE.DAT` file.
PRIORITY.SEM	Forces MDaemon to reload the `PRIORITY.DAT` file.
EXCPTION.SEM	Forces MDaemon to reload the `EXCPTION.DAT` file.
APPLYNOW.SEM	Causes the same action that occurs when you press the APPLY NOW button in the Primary Domain Setup screen. This is required when changes are made to the port, domain name/IP or bind settings.

HANGUPR.SEM Forces a “rude” hang-up of a connected RAS session. This is an immediate and unconditional hang-up without regard to mail sessions which may be in progress across the connection so watch out!

HANGUPG.SEM Forces a “graceful” hang-up of a connected RAS session. MDaemon will wait for any pending mail sessions to close and will then hang-up the RAS session.

QUEUERUN.SEM Just before a mail session begins MDaemon will create this semaphore file. Inside the file will be a datestamp indicating the time and date of the most recent mail processing interval.

ONLINE.SEM MDaemon will create this semaphore file once it makes a successful connection using RAS to the ISP. MD will remove the semaphore once the connection has been terminated. This is useful if you want to know when MD is using the RAS sub-system.

PREDIAL.SEM MDaemon will create this file just before trying to use RAS/DUN. This will allow other software to detect when it should free the dialup port so that MDaemon can use it.

POSTDIAL.SEM MDaemon will create this file immediately after a connection made by MDaemon is taken down.

REBOOTMD.SEM MD will reboot the tray icon and make the interface accessible. This is useful if you are running MD as a service and the interface is not present.

FWUNLESS.SEM Reloads the Forward Exception database.

DLUNLESS.SEM Reloads the Delete Exception database.

DVUNLESS.SEM Reloads the Delivery Exception database.

SUPPRESS.SEM Reloads the suppressed address list for all domains.

MSGID.SEM Forces a reload of the Dedupe value list.

GRPLIST.SEM Reloads Mailing List names dynamically.

CATLIST.SEM Reloads Catalog names dynamically.

WATCHDOG.SEM MDaemon will check for and remove this semaphore from the APP directory at approximately 10-20 second intervals. This file can be used by external apps to check if MDaemon is running. If this file remains in the APP directory for more than 20 seconds, that is a good indication that MDaemon is no longer running.

Appendix B

Message Precedence System

This feature makes it possible for you to assign a "Precedence" value (level of importance) of 0 to 99 to messages. This value signifies the relative sort order of the messages during the delivery process. The lower the value, the higher its importance and the further up it will be in the sort order within a message queue. Thus, MDaemon will attempt to deliver a message with a value of 10 before one with a value of 90. As a guideline for assigning Precedence values: 10 = Urgent, 50 = Normal, and 80 = Bulk.

You will find controls related to this feature on the Headers tab of Miscellaneous Options (page 199) and on the Options tab of the Mailing List Editor (page 269). You can also use the "Add Extra Header Item To Message" action of the Content Filters (page 168) to insert the `Precedence` header into any message.

Appendix C

Creating an SMTP Session Policy Statement

More and more sites these days are announcing an up front policy regarding relaying of SMTP mail during the SMTP session itself. If you would like to have MDaemon send a statement to the remote SMTP client when it attempts to send a message to your site you can do so by placing a text file called POLICY.DAT in the \app\ directory. The content of this file will be sent to the remote SMTP client immediately after the SMTP greeting. For example, a POLICY.DAT file with a statement regarding relaying of mail would look like this during the SMTP transaction:

```
220-Alt-N Technologies ESMTP MDaemon v6
220-This site does not authorize you to relay mail.
220-If you are not an authorized user of our domain’s mail
220-server you must
220-not relay mail through this site.
220
HELO domain.com
and so on...
```

The POLICY.DAT file must be comprised of printable ASCII text only and have no more than 512 characters per line; however no more than 75 characters per line is highly recommended. The maximum size of this file is 5000 bytes. MDaemon will not display files larger than 5000 bytes. Each line within this file must start with “220-” except the last line which must start with “220 “ (note that the dash is missing on the last line and is replaced with a blank space).

For example:

```
C:\MDAEMON\APP>Copy con POLICY.DAT
220-This site does not authorize you to relay mail.
220 So don’t do it!
^Z
```

Appendix D

Customizing SMTP and POP Protocol Strings

MDaemon contains a mechanism for altering the SMTP and POP protocol strings that it uses. You can provide custom strings for most of the SMTP and POP dialog. Each string that MDaemon uses has a unique number and a specific default value. These defaults will be used unless a custom string is found in the [Custom-SMTP] or [Custom-POP] sections in the MDAEMON.INI file.

When creating custom SMTP strings, pay close attention to the following:

1. Some SMTP default strings start with a blank space character (see chart below). Any replacement for these strings must also start with a blank space character. **Failure to do so will result in server failure!**

2. You must enclose the custom string in quotation marks when you place it into the `mdaemon.ini` file. **Failure to do so will result in server failure!**

3. Some strings contain macros such as "%s" or "%d". These macros are dynamically filled in with data when the string is loaded and used. Custom strings are not required to use these macros. However, a custom string may duplicate these macros provided they are placed in the same sequence as they appear in the default string. **Failure to place macros in the same sequence within a custom string will result in instant server failure!**

When creating custom POP strings, pay close attention to the following:

1. All POP default strings start with either "`+OK`" or "`-ERR`" (see chart below). Any replacement for these strings must also start with "`+OK`" or "`-ERR`". **Failure to properly use "`+OK`" or "`-ERR`" text at the start of a custom string will result in server failure!**

2. Some strings contain macros such as "%s" or "%d". These macros are dynamically filled in with data when the string is loaded and used. Custom strings are not required to use these macros. However, a custom string may duplicate these macros provided they are placed in the same sequence as they appear in the default string. **Failure to place macros in the same sequence within a custom string will result in instant server failure!**

Here is a list of the unique numbers and default string values used by MDaemon. Only the following strings can be changed. **Attempting to change a string that is not listed here will result in server failure!**

SMTP STRING CODES

```
7000="%s ESMTP service ready [%d]"
7002="%s Hello %s, pleased to meet you"
7004="<%s>, Sender ok"
7062="<%s>, Sender ok (alias for %s)"
7006="<%s>, Recipient ok"
7008="<%s>, Recipient ok (alias for %s)"
```

```
7010=“Enter mail, end with <CRLF>.<CRLF>“
7011=“See ya in cyberspace”
7012=“What? I don’t understand that.”
7013=“Ok, message saved”
7014=“%s is not a valid maildrop.  Please check the address and try again.”
7015=“Sorry, try later.  Can’t create temporary mail file. :(“
7016=“RSET?  Well, OK.”
7017=“Why is there an NOOP instruction?”
7018=“Yeah, I know that one.  He (or she) is %s <%s>.”
7019=“<%s>?  Never heard of ‘em.”
7020=“<%s>?  There’s more than one possible match to that query on this
      server.”
7021=“Yeah, there’s a list here by that name.  Mail to <%s>.”
7022=“<%s>?  There’s no mailing list here by that name.”
7023=“<%s>?  There’s more than one possible match to that query on this
      server.”
7024=“Hey!  I don’t let remote systems TURN on me.”
7025=“Help system currently inactive.”
7033=“%s Hello %s, did you know your name is really %s?”
7034=“Unexpected command or sequence of commands.”
7037=“Sorry, SMTP server too busy right now (%d).  Try again later.”
7038=“SMTP session successful, %ld bytes transferred!”
7039=“SMTP session abnormally terminated, %ld bytes transferred!”
7041=“Sending <%s> to [%s]”
7042=“Connection timed out!”
7043=“Spooling mail to default gateway”
7044=“This server does not accept routed mail”
7046=“Node <%s> does not store mail here”
7047=“Your IP address <%s> does not have access to node <%s>“
7048=“No messages waiting for node <%s>“
7050=“<%d> pending messages for node <%s> started”
7051=“Unable to queue message for node <%s>: Internal processing error”
7052=“This server configured to NOT honor EHLO at present.”
7053=“Sorry, <%s> is not allowed access from your location”
7055=“<%s>, Sender unknown”
```

You can see from the table that the initial SMTP greeting string is coded 7000. Therefore to create a custom SMTP greeting string place the following entry into the MDAEMON.INI file:

```
[Custom-SMTP]
7000=“ Alt-N Technologies ESMTP server”
```

Note that you must enclose the custom string in quotations. Note also that this example string does not use any %s macros like the default one does. This is fine.

POP STRING CODES

```
7200=“+OK %s POP service ready [%d]”
7201=“+OK %s... Recipient ok”
7235=“-ERR Access denied.  Contact postmaster@%s for more information.”
7234=“-ERR sorry, POP server too busy right now.  Try again later.”
7202=“-ERR sorry, there’s no mailbox for %s here”
7203=“-ERR that command is valid only in the AUTHORIZATION state!”
7204=“-ERR that command is valid only in the TRANSACTION state!”
7205=“-ERR that command is valid only in the UPDATE state!”
```

```
7233=“-ERR maildrop already locked”
7206=“+OK %s... see ya in cyberspace”
7207=“-ERR access denied”
7208=“+OK %s’s mailbox has %d total messages (%ld octets).”
7210=“+OK %d messages (%ld octets)”
7219=“-ERR no such message”
7220=“-ERR no such message, only messages 1 thru %d are present in your
      inbox”
7222=“+OK %s %s POP Server signing off (mailbox empty)”
7223=“+OK %s %s POP Server signing off (%d messages left)”
7214=“-ERR unknown POP command!”
7213=“+OK message %d deleted”
7224=“-ERR message %d already marked for deletion”
7216=“Sending TOP of message %d (unbuffered operation…)”
7241=“Sending <%s> to [%s]”
7242=“Connection timed out!”
7243=“Transmission Complete <%s>“
7247=“Message %d (%ld bytes) exceeds max message size limit of %ld bytes”
7248=“Collecting Message %d (%ld bytes) would exceed account’s max disk space
      limit of %ld bytes”
7249=“Collecting Message %d would exceed account’s max stored message limit
      of %ld”
7237=“POP session complete, %ld bytes transferred!”
7238=“POP session timed out, %ld bytes transferred!”
```

Appendix E

Route Slips

The concept of a “route slip” has been present in MDaemon since the beginning but has never been documented. Typically, a message file that is waiting in a queue contains within itself all the information that is needed to get the message delivered to the proper location. There are headers stored within the .MSG file (such as the X-MDaemon-Deliver-To header) which provide MDaemon with instructions as to where and to whom the message should be delivered. Sometimes however it is necessary or useful to override this information and provide specific alternatives to where and to whom an .MSG file must be sent. The route slip provides just such a mechanism. A route slip is a file which provides MDaemon with very specific instructions as to where and to whom a message file should be sent. If a route slip is present for a particular message file then the settings within the route slip - and not those within the .MSG file itself - control where and to whom the message is sent.

Route slips end with the extension .RTE. For example, if a message file waiting to be sent is called MD0000.MSG then the corresponding route slip file for this message will be called MD0000.RTE and must be located in the same directory (mail queue) as the message file.

The format of a route slip is as follows:

```
[RemoteHost]
DeliverTo=remote-domain.com
```

This section of a route slip provides MDaemon with the server to which the corresponding .MSG file is to be sent. MDaemon will always attempt a direct connection to this host attempting to route the message in as short a time as possible. Only one host may be specified.

```
[RemoteHost]
IgnoreRcptErrors=Yes (or No)
```

It is possible to specify an unlimited number of recipients of the .MSG file being sent. Sometimes hosts might refuse a particular address to which you are attempting to send a copy of the message. Ordinarily under SMTP regulations the session should be aborted. This switch will allow MDaemon to proceed to the next recipient in the list without aborting the session completely.

```
[Port]
Port=xxx
```

This switch specifies the port that the TCP/IP connection and delivery attempt should be made on. 25 is the default for SMTP email.

```
[LocalRcpts]
Rcpt0=address@my-domain.com
Rcpt1=other-address@my-domain.com
Rcpt2=yet-another-address@my-domain.com
```

```
[RemoteRcpts]
Rcpt0=address@foreign-domain.com
Rcpt1=other-address@foreign-domain.com
Rcpt2=yet-another-address@foreign-domain.com
```

These sections of the route slip allow you to specify any number of local and remote recipients who should receive a copy of the associated .MSG file. Local and remote recipient addresses must be kept separate and placed in their corresponding [LocalRcpts] and [RemoteRcpts] sections.

Route slips provide a good mechanism for delivering or redirecting email but they are not generally necessary. One use that MDaemon makes of route slips is in the case of “routed” mailing list mail. When you have a mailing list that is set to route a single copy of the list message to some remote host a route slip is employed to accomplish this. It is a very efficient method of mail delivery when you have bulk addresses to deliver mail to since only a single copy of the message is required while any number of recipients of the message can be specified. Not all remote hosts allow this sort of routing to occur however. Since it is ultimately they who will have to deliver a copy of the message file to each address some hosts place an upper limit on the number of recipients they will allow you to specify.

Appendix F

MDaemon Technical Support

Technical Support for the MDaemon Server is provided by Alt-N Technologies and is offered on several different levels, outlined below. Please review the support options and select whichever is appropriate for your needs.

All of the following options are located and fully discussed at the MDaemon web site.

```
http://www.mdaemon.com
```

Telephone Support for All Users

MDaemon Technical Support is available via telephone for a per incident flat rate fee of $60.00. Paid telephone support is available between the hours of 9:00am and 6:00pm, Central Standard Time, Monday through Friday (excluding holidays), at (817) 652-0204. When calling, please have credit card information ready.

Free Technical Support Options

Support for all users is provided via the MDaemon Help Desk and the MDaemon Open Discussion Forum, which allows for dialog within a threaded, searchable, and intuitive forum environment.

- **MDaemon Help Desk**— http://www.altn.com/Support/Default.asp?product_id=MDaemon

  The MDaemon Help Desk outlines a number of resources to help you learn more about MDaemon, troubleshooting problems, and so on. By utilizing the Help Desk you can often avoid the need to contact Technical Support. The MDaemon Help Desk contains a number of useful resources including:

  MDaemon Knowledge Base— You can search our support database for answers to your questions. With support for time-based, natural language, and article-based searching, plus a listing of Frequently Asked Question, you're sure to find the right answer!

  Helpful Articles— The Help Desk contains a number of useful articles addressing various MDaemon configuration issues and other related topics.

  Free Add-on & Complimentary Software— Here you can download free supplementary software and utilities written by MDaemon's developers and users.

- **MDaemon Support Mailing List**—The MD-Support email discussion group is a mailing list hosted by Alt-N Technologies. It is an open membership list where users can get help and discuss MDaemon with other users. MDaemon's Development Team, other support staff, and a large mix of MDaemon users regularly participate in the discussion and contribute feedback and help. Odds are that someone will have an answer to your MDaemon question in the MD-Support email group. To join **MD-Support**, send a message to **mdaemon@altn.com** with the following in the first line of the body:

SUBSCRIBE md-support@altn.com myaddress@mydomain.com

- **MDaemon Open Discussion Forum**— Come join in the MDaemon Open Discussion Forum to get help on your questions from both the MDaemon Tech Support Staff and other MDaemon users. It's a great way to learn, share, and exchange ideas! The Forum allows for dialog within a threaded, searchable, and intuitive forum environment. It is located at

  ```
  http://lists.altn.com
  ```

- **Free Email Support for All Users**— Free Unlimited Email Support is available for all MDaemon users. To obtain this free support via email, please submit your technical support request using the Technical Support Request Form located at:

  ```
  http://www.altn.com/Support/Default.asp?product_id=MDaemon
  ```

  The Technical Support Request Form can also be reached via link from the MDaemon web site.

Reseller Purchase

Users who purchased their copy of MDaemon from an Official Alt-N Partner will be referred back to them for support. If you would like to receive technical support from Alt-N Technologies, you will be required to pay the telephone support charge for a per incident flat rate fee of $60.00.   For information about Official Alt-N Partners, or to locate a reseller near you visit:

```
http://www.altn.com/Partners/
```

Sales and Reseller Inquiries

Sales questions (of a non-technical nature) relative to MDaemon software should be directed to <**sales@altn.com**>. Alternatively, you can call Alt-N Technologies at (817) 652-0204.

Contacts

MDaemon, WorldClient, and RelayFax are trademarks of Alt-N Technologies, LTD.

Alt-N Technologies, LTD.

1179 Corporate Drive West, Suite #103
Arlington, TX 76006
http://www.altn.com
817-652-0204
817-652-0009 fax

Sales and Reseller Inquiries

Sales questions (of a non-technical nature) relative to MDaemon software should be directed to <**sales@altn.com**>. Alternatively, you can call Alt-N Technologies at (817) 652-0204.

You can locate an MDaemon reseller near you by using the Alt-N partner Database located at:

```
http://www.altn.com/partners/
```

Documentation Issues

mdaemon-docs@altn.com

MDaemon Beta Testing

Alt-N Technologies maintains an open policy on Beta-team participation. If you would like to join Alt-N's Beta-test Team and receive advance beta-copies of future MDaemon releases, Service Packs, and other Alt-N software, simply send a message to mdaemon@altn.com with the following in the first line of the body:

SUBSCRIBE md-beta@altn.com myaddress@mydomain.com

Our system will return an information packet to you with instructions for obtaining Beta software and participating in Beta testing. For more information on the **MDaemon Beta Team** visit:

http://www.altn.com/Beta/Default.asp

Note

The Beta Team is for those who wish to acquire Alt-N software before its general release and aid in its testing; it is not a technical support alternative. Technical support for MDaemon will only be provided through those methods outlined in the **MDaemon Technical Support** section. If you would like to subscribe to the MDaemon support Mailing List hosted by Alt-N Technologies, send a message to mdaemon@altn.com with the following in the first line of the body of the message and you will be added to the mailing list:

SUBSCRIBE md-support@altn.com myaddress@mydomain.com

Glossary

ACL—Stands for **A**ccess **C**ontrol **L**ists. ACL is an extension to the Internet Message Access Protocol (IMAP4) that makes it possible for you to create an access list for each of your IMAP message folders, thus granting access to your folders to other users whom also have accounts on your mail server. Further, you can set permissions governing the extent to which each user has control over those folders. For example, you can designate whether or not a user is allowed to delete messages, flag them as read or unread, copy messages to folders, create new subfolders, and so on. Only email clients that support ACL can be used to share this access and set permissions. However, if your email client doesn't support ACL you can still set these permissions from the MDaemon version 6 GUI. Right now very few email clients support ACL directly but there is an excellent utility from www.bynari.net called InsightConnector that will add this functionality (and more) to Microsoft Outlook.

ACL is fully discussed in RFC 2086, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2086.txt
```

ASCII—Pronounced as-key, ASCII is an acronym for "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". It is the worldwide standard code for representing all upper and lower-case Latin letters, numbers, and punctuation as a 7 digit binary number, with each character assigned a number from 0 to 127 (i.e. 0000000 to 1111111). For example, the ASCII code for uppercase M is 77. The majority of computers use ASCII codes to represent text, which makes it possible for them to transfer data to other computers. Most text editors and word processors are capable of storing files in ASCII format (sometimes called ASCII files). However, most data files—particularly those containing numeric data—are not stored in ASCII format.

Several larger character sets have 128 additional characters because they use 8 bits instead of 7. These extra characters are used to represent symbols and non-English characters. The DOS operating system uses a superset of ASCII called extended ASCII or high ASCII. A standard that is closer to universal, however, is ISO Latin 1, which is used by many operating systems and Web browsers.

ATRN—See ETRN and ODMR below.

Attachment—A file attached to an email message. Most email systems only support sending text files as email, therefore if the attachment is a binary file or formatted text file (e.g. a word processor document), it must first be encoded as text before it is sent and then decoded once it is received. There are a number of encoding schemes—two of the most prevalent being Multipurpose Internet Mail Extensions (MIME) and Unix-to-Unix encode (Uuencode). For incoming messages, Alt-N's MDaemon server can be configured to either leave the decoding process to the recipient's email client or automatically decode attachments and store them in a specific location before delivering the message to the local user.

Backbone—A line or series of connections that form the major pathway within a network. This term is relative since the non-backbone lines in a large network might be larger than the backbone in a smaller network.

Bandwidth—The amount of data that can be transmitted in a fixed amount of time through a network or modem connection, usually measured in bits-per-second (bps). A full page of English text is about 16,000 bits, which a fast modem could transfer in about 1 to 2 seconds. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

A good illustration of bandwidth is a highway. The highway represents the connection while the cars traveling on it represent the computer data. The wider the highway (the greater the bandwidth) the more cars that will be able to travel on it.

Baud—Baud rate is a measure of how frequently carrier signals change value on a phone line. It is a reference to the speed at which a modem transmits data. Usually, slower modems are described in terms of Baud rate while higher speed modems are described in bits per second. "Baud rate" and "bits per second" are not necessarily synonymous terms since each signal can encode more than one bit in high-speed connections.

Bit—A single **B**inary dig**it**. It is the smallest unit of computer data; a single digit number in base-2 (i.e. 0 or 1). It is usually abbreviated with a lower case "b" as in "bps" (bits per second). A full page of text is approximately 16,000 bits.

Bitmap—Most pictures you see on your computer, including all the ones found on the Internet, are bitmaps. A bitmap is a really just a map of dots (or bits) that looks like a picture as long as you're not to close to the screen, or have the bitmap magnified too much, to see the shape they make. Common Bitmap file types include BMP, JPEG, GIF, PICT, PCX, and TIFF. Because bitmap images are made up of a bunch of dots, if you zoom in on a bitmap it looks blocky rather than smooth. Vector graphics (usually created in CorelDraw, PostScript, or CAD formats) scale up much better because they are geometric shapes generated mathematically rather than simply being made of seemingly "random" dots.

Bps—"**B**its **P**er **S**econd" is a measurement of how fast computer data can be moved from one place to another. For example, a 33.6 kbps modem can transfer 33,600 bits per second. Kilobits (1000 bits) per second and megabits (1.000,000 bits) per second are abbreviated "Kbps" and "Mbps" respectively.

Browser—Short for "Web browser", it is an application used to display web pages. It interprets HTML code, text, hypertext links, images, JavaScript, and so on. The most widely distributed browsers are Internet Explorer and Netscape Communicator.

Byte—A set of bits (usually eight) that represent a single character. There are 8 bits in a byte, sometimes more, depending on how the measurement is being made. "Byte" is abbreviated with an uppercase "B".

Cache—Pronounced like "cash". There are various types of caches, but all are used to store recently used information so that it can be accessed quickly later. For example, a web browser uses a cache to store the pages, images, URLs, and other elements of web sites that you have recently visited. When you return to a "cached" page the browser will not have to download these elements again. Because accessing the cache on your hard disk is much faster than accessing the Internet, this significantly speeds up browsing.

MDaemon's IP Cache stores the IP addresses of domains to which you have recently delivered messages. This prevents MDaemon from having to lookup these addresses again when delivering additional messages to the same domains. This can greatly speed up the delivery process.

CGI—Common **G**ateway **I**nterface is a set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. However, a CGI program is usually a small program that takes data from a web server and does something with it, like putting the content of a form into an email message, or doing something else with that data. CGI programs are often stored in a web site's "cgi-bin" directory and therefore appear in a URL that accesses them, but not always.

cgi-bin—The most common name of the directory on a web server in which CGI programs are stored. The "bin" part of "cgi-bin" is short for "binary" because most programs used to be referred to as "binaries". In reality, most cgi-bin programs are text files; scripts executed by programs located elsewhere.

CIDR—"**C**lassless **I**nter-**D**omain **R**outing" is a new IP addressing system that replaces the older system, which was based on classes A, B, and C. CIDR IP addresses look like normal IP addresses followed by a slash and number, called the IP prefix. For example:

123.123.0.0/12

The IP prefix defines how many addresses are covered by the CIDR address, with lower numbers covering more addresses. In the above example, the IP prefix of "/12" can be used to address 4,096 former Class C addresses.

CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

CIDR is addressed in RFCs 1517-1519, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc1517.txt
http://www.rfc-editor.org/rfc/rfc1518.txt
http://www.rfc-editor.org/rfc/rfc1519.txt
```

Client—A software program that is used to contact and obtain data from or send data to a *server* software program. The server is usually located on another computer, either on your local network or at some other location. Each *client* program is designed to work with one or more specific kinds of *server* programs, and each server requires a specific kind of client. A web *browser* is a specific kind of client that communicates with web *servers.*

Common Gateway Interface—See CGI above.

Cookie—In computer terminology, a *cookie* is data sent by a web server to your web browser, which is saved and later used for various purposes when you return to the same site or go to another location on the site. When a web server receives a request from a web browser that includes a cookie, it is able to use the information the cookie contains for whatever purpose it was designed, such as customizing what is sent back to the user, or for keeping a log of the user's requests. Typically, cookies are used for storing passwords, usernames, preferences, shopping cart information, and similar things related to the site to which they correspond so that the site can appear to "remember" who you are and what you've done there.

Depending on your browser's settings, you may accept or not accept the cookies, and save them for various amounts of time. Usually cookies are set to expire after a predetermined amount of time and are saved in memory until the web browser software is closed down, at which time they may be saved to disk.

Cookies **cannot** read your hard drive. They can, however, be used to gather information about you related to your usage of their particular web sites, which would be impossible without them.

Dial-up Networking—A component in Windows that enables you to connect your computer to a network via a modem. Unless your computer is connected to a Local Area Network (LAN) with access to the Internet, you will need to configure Dial-Up Networking (DUN) to dial a Point of Presence (POP) and log on to your Internet Service Provider (ISP) before you will have Internet access. Your ISP may need to provide certain information, such as the gateway address and your computer's IP address.

DUN is accessed through the My Computer icon. A different dialup profile can be configured for each online service that you use. Once configured, you can copy a profile shortcut to your desktop so that all you need to do to make a connection is double-click the connection icon.

Default—This term is used to refer to the preset value for options in computer programs. Default settings are those settings which are used when no specific setting has been designated by the user. For example, the default font setting in Netscape Communicator is "Times". This setting will remain "Times" unless you change it to something else. Default settings are usually the value that most people will choose.

Frequently the term *default* is also used as a verb. If a custom setting won't work or the program lacks some needed bit of data for completing a task, it will usually "default" to a specific setting or action.

DHCP—An acronym for "**D**ynamic **H**ost **C**ontrol **P**rotocol". Network servers use this protocol to dynamically assign IP addresses to networked computers. A DHCP server waits for a computer to connect to it and then assigns it an IP address from a stored list.

DHCP is addressed in RFC-2131, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2131.txt
```

Domain Gateway—See Gateway below.

Domain Name—This is the unique name that identifies an Internet web site. For example, "altn.com" is the domain name of Alt-N Technologies. Each domain name contains two or more parts separated by dots; the leftmost part is the most specific while the rightmost part is the most general. Each domain name also points to the IP address of a single server, but a single server may have more than one domain name. For example, "mail.altn.com", "alt-n.com", and "somedomain.com" could all point to the same server as "altn.com", but "altn.com" could not point to two different servers. There are, however, methods for designating alternate servers to which clients will be directed if the main server goes down or is otherwise unavailable.

It is also common for a domain name to be registered but not be connected to an actual machine. The usual reason for this is the domain name's owner hasn't created a web site yet, or so that they can have email addresses at a certain domain without having to maintain a web site. In the latter case, there must be a real Internet machine to handle the mail of the listed domain name.

Finally, it is common to see the term "domain name" shortened and referred to as simply "domain". The word "domain" has other meanings and can refer to other things, such as a Windows NT domain or a class of values, so you should be aware of the distinction in order to avoid confusion.

Domain Names are addressed in RFCs 1034-1035, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc1034.txt
http://www.rfc-editor.org/rfc/rfc1035.txt
```

DomainPOP—Developed by Alt-N Technologies to be a part of the MDaemon server, DomainPOP makes it possible to provide email services for an entire LAN or workgroup from a single ISP POP mailbox. In the past, unless a company's email server had on constant "live" connection to the Internet, the only way to provide Internet email services to a workgroup was for each person to have their own mailbox on the company's ISP from which they could collect their mail. With DomainPOP only a single mailbox is required. The ISP pools all mail for the company's domain name into the mailbox from which it is periodically collected by DomainPOP. Then, DomainPOP parses the messages to determine the intended recipients of each and distributes them to the appropriate local user mailboxes. Thus email is provided for an entire network from a single dialup ISP account.

Download—The process by which your computer retrieves or obtains data from another computer. For example, information is obtained from the Internet by *downloading* it from other computers. The reverse of this is *uploading*. If you wish to send information to another computer then you will *upload* it to them.

Driver—A small program that communicates with a certain hardware device. Drivers contain information needed by the computer and other programs to control and recognize the device. Windows-based computers often have drivers packaged as a dynamic link library (DLL) file. Most hardware devices used with Macs do not need drivers, but when a driver is necessary it will usually come in the form of a System Extension.

DUN—See Dial-up Networking above.

Email—Stands for **"**Electronic mail". This term also appears in the forms: "E-mail", "e-mail", and "email"; all have the same meaning. Email is the transmission of text messages over communications networks. Most computer networks have some form of email system. Some email systems are confined to a single computer network, but others have gateways to other networks (which enables them to communicate with multiple locations), or to the Internet (which enables them to send email anywhere in the world).

Most email systems include some form of *email client* (also referred to as a *mail client* or just *client*) which contains a text editor and other tools for composing messages, and one or more *servers* which receive the email from the clients and route it to its appropriate destination. Typically, a message is composed using the client, passed to a server for delivery to the *email address* (or addresses) specified in the message, and then routed by the server to another server that is responsible for storing messages destined for that address. If the message's destination is a local address for which the original server is responsible then it may be stored on the original server rather than routed to another. Last, the recipient of the message will connect to their server and retrieve the message by using their email client. This entire process of transferring an email message from your client to its destination server usually only takes a few seconds or minutes.

Besides containing simple text, email messages may also include file *attachments*. These attachments can be any type of file that you desire: pictures, text files, program files, other email messages, and so on. However, since most email systems only support sending text files, attachments must first be encoded (converted to a text format) before they can be sent, and then decoded when they arrive at their final destination. This process is usually done automatically by the sending and receiving mail clients.

All Internet Service Providers (ISPs) offer email. Most also support gateways so that you can exchange email with users of other email systems. Although there are many different protocols used for processing email by many different email systems, several common standards make it possible for users on virtually all systems to exchange messages.

Email Address—A name or string of characters that identifies a specific electronic mailbox on a network to which email can be sent. Email addresses are the locations to and from which email messages are sent. Email servers need email addresses so that they can route messages to their proper destinations. Different types of networks have different formats for email addresses, but on the Internet all email addresses have the form: “mailbox@domain.com”.

For example,

Frank.Thomas@altn.com

Email Client—Also called a *mail client* (or just *client*), an *email client* is a software application that enables you to send, receive, and organize email. It is called a client because email systems are based on client-server architecture; a client is used to compose the email and then send it to a server, which then routes it to the recipient’s server from which it will be retrieved by the recipient’s client. Usually, email clients are separate software applications installed on the user’s machine, but products such as Alt-N Technologies’ WorldClient Server contain a built in client that is “served” to the user’s web browser. Thus, their browser is used as the client rather than needing to install one on their machine. This greatly enhances the portability and convenience of email.

Encryption—A security measure, *encryption* is the coding or scrambling of information in a file so that it will only be intelligible when it has been decoded or decrypted. Encryption is frequently used in email so that if a third party intercepted the email they would not be able to read it. The message is encrypted when it is sent and then decrypted at its final destination.

Ethernet—The most common type of connection used in a Local Area Network (LAN). Two of the most widely used forms of Ethernet are 10BaseT and 100BaseT. A 10BaseT Ethernet can transfer data at speeds up to 10 mbps (megabits per second) through a cable or wireless connection. A 100BaseT Ethernet transfers data at speeds up to 100 mbps. A Gigabit Ethernet can transfer data at rates up to 1000 mbps and is employed by some Apple computers.

ETRN—An acronym meaning **E**xtended **T**U**RN**. It is an extension to SMTP that enables an SMTP server to send a request to another SMTP server to send, or “dequeue”, mail that is being held for it. Because SMTP by itself cannot request mail (email is usually requested via the POP or IMAP protocols), this makes it possible for the SMTP server making the ETRN request to cause the remote server to start an SMTP session and begin sending the stored email to the host specified in the request.

The `TURN` command used for this purpose posed a security risk because it caused the SMTP session to reverse direction and begin sending the stored mail immediately without any verification or authentication that the requesting server was actually who it claimed to be. `ETRN` starts a new SMTP session rather than reversing direction. Thus if the server making the request is a "spoofed" host, the sending server will still attempt to deliver the mail to the real host instead. There is now a proposed standard that introduces Authenticated TURN (`ATRN`), which, like `TURN`, reverses the direction of the SMTP session but requires authentication before doing so. This new standard is On-Demand Mail Relay (ODMR). Alt-N Technologies' MDaemon server supports both ETRN and ODMR's ATRN.

ETRN is addressed in RFC 1985, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc1985.txt
```

ODMR is addressed in RFC 2645, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2645.txt
```

FAQ—Pronounced together as "fack" or as separate letters "F-A-Q", FAQ stands for "**F**requently **A**sked **Q**uestions". FAQs are documents that provide answers to the most commonly asked questions on a given subject. They usually appear in some form of list format with each question listed first followed by its answer. In larger FAQs, oftentimes all of the questions will be listed at the beginning of the document with references (or hyperlinks, in online FAQs) to the location of the question and answer in the document. FAQs are frequently used as a starting point for technical support and instructions—a great deal of time and effort can be saved if you have access to a FAQ that answers your question instead of being forced to contact technical support.

File Transfer Protocol—See FTP below.

Firewall—In computer terminology, a *firewall* exists when you undertake security measures, through either software or hardware means, to separate a computer network into two or more parts, or otherwise limit access to it to certain users. For example, you might want to let everyone view the home page of a web site hosted on your network but allow only your employees to get to an "employee only" area. Regardless of the method that you use to accomplish this—requiring a password, allowing connections from only certain IP addresses, or the like—the employee area is said to be behind a firewall.

FTP—Acronym for "**F**ile **T**ransfer **P**rotocol." It is a common and efficient method of transferring files via the Internet from one computer to another. There are specific client/server applications designed for this purpose called "FTP servers" and "FTP clients"—FTP Voyager and CuteFTP are two of the most common clients. Usually FTP clients can perform quite a few other functions besides simply transferring files and are thus highly useful products. Some web browsers also contain support for File Transfer Protocol, though sometimes for downloading only. Additionally, most FTP servers are "anonymous FTP", which means that anyone can log in to them in order to download files—usually by specifying "anonymous" as the user name and then your email address as the password. Oftentimes you can download files from anonymous FTP sites without having to log in at all—they can be retrieved by simply clicking on a link. For browsers that support FTP, usually all that needs to be done is to connect to the FTP site using "ftp://…" in its URL rather than "http://…"

FTP is addressed in RFC-959, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc959.txt
```

Gateway—Computer hardware or software that translates data between two applications or networks with protocols that are dissimilar. "Gateway" is also used to describe any means by which access is provided from one system to another. For example, your ISP is a gateway to the Internet.

Alt-N Technologies' MDaemon email server can function as an email gateway for other domains through the use of its Domain Gateways feature. It acts as an intermediary, or Gateway, by collecting the domain's email and then holding it until the domain collects it. This is useful both for domains that do not maintain a continuous connection to the Internet and for domains that require a backup server in case theirs goes down.

GIF—"**G**raphics **I**nterchange **F**ormat" is a popular format for image files and is the most common format of images found on the Internet. GIF uses indexed colors or a palette of a certain number of colors, which greatly reduces file size—especially when the image contains large areas of the same color. The reduced size enables them to be quickly transferred between systems and accounts for their popularity on the Internet. The GIF compression formula was originally developed by CompuServe and thus you will often see GIF referred to as CompuServe GIF.

Graphical User Interface—See GUI below.

GUI—Pronounced "gooey", this acronym stands for "**G**raphical **U**ser **I**nterface". A GUI makes it possible to interact with your computer or application by using a pointing device to click graphical elements on the screen rather than typing in text at a command line. The Microsoft Windows and Apple Mac operating systems are both GUI-based, but—although first introduced by Apple—the idea of a graphical user interface actually originated from Xerox.

Host—Any computer on a network that acts as a server for other computers on the same network. The host machine may be running a web server, email server, or other services, and it is common for it to provide several services at once. Host is also often used in the verb form "to host". For example, a machine running an email server would be "hosting" the email.

On peer-to-peer networks it is common for machines to be both hosts and clients at the same time. For example, your machine may host your network's printer but also be used by you as a client to collect email and download files from another host.

HTML—An acronym for "**H**yper**t**ext **M**arkup **L**anguage. It is the coding language used to create Hypertext documents used on the World Wide Web. Simply put, an HTML document is a plain text document that contains formatting codes and tags that the user's web browser interprets and presents as a web page complete with formatted text and colors. For example, a browser receiving an HTML document containing the text "<B>Text</B>" would present the word "Text" in Bold. Because plain text files are very small, this makes it possible for them to be quickly transferred over the Internet.

HTTP—Hyper**t**ext **T**ransfer **P**rotocol (HTTP) is the protocol used for transferring *hypertext* files between computers over the Internet. HTTP requires a client program on one end (usually a web browser) and an HTTP server on the other end.

HTTP is addressed in RFC-2616, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2616.txt
```

Hypertext—Any text that contains a hyperlink or jump to another document or place within the same document is called hypertext. Sometimes the text is also called a hypertext link or simply link. Hypertext can be either a word or phrase and has the link embedded in it so that clicking it will move you to the "book marked" location or cause the linked document to be displayed. Usually hypertext links are apparent because the text is underlined and a different color, but that is not required. Sometimes hypertext will look no different than normal text, but will almost always be indicated by some sort of graphical change to your pointer when the mouse pointer is paused over it.

Hypertext Markup Language—See HTML above.

IMAP—Developed by Stanford University, **I**nternet **M**essage **A**ccess **P**rotocol (IMAP) is a protocol used for managing and retrieving email messages. The latest version is IMAP4 and is similar to POP3 but with a number of additional features. IMAP4 is best known as a protocol used for managing email messages on the server rather than on the user's local machine—messages can be searched for keywords, organized in folders, specifically selected for downloading, and other features, all while they are still on the server. Thus IMAP places less demand on the user's machine and centralizes email so that it can be accessed from multiple locations.

IMAP is addressed in RFC-2060, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2060.txt
```

IMAP4 ACL extension—See ACL above.

Internet—The Internet was created in 1969 by the United States military, originally to be a communications network that couldn't be destroyed during a nuclear war. It now consists of millions of computers and networks all over the world. By design, the Internet is decentralized—it is not controlled by any company, organization, or country. Each host (or machine) on the Internet is independent of the others and can provide whatever information or services its operators wishes to make available. Nevertheless, most information transferred over the Internet at some point passes through "backbones", which are extremely high-bandwidth high-speed connections controlled by the largest Internet Service Providers and organizations. Most people access the Internet through an online service such as AOL or through an Internet Service Provider (ISP) that maintains or is connected to one of these backbones.

Many people believe that the *World Wide Web* (WWW) and the Internet are the same thing, but this is not the case. The WWW is only one part of the Internet not the Internet itself. It is the most visible and popular part, largely driven by commerce, but still only a part.

Intranet—Simply put, an intranet is a small or private Internet used strictly within a company or organization's network. Although intranets vary widely from organization to organization, they may contain any of the features available on the Internet. They may have their own email systems, file directories, web pages to be browsed, articles to be read, and so on. The primary difference between an intranet and the Internet is that an intranet is relatively small and confined to an organization or group.

IP—An acronym for "**I**nternet **P**rotocol" (e.g. as in TCP/IP). Internet protocols make it possible for data to be transferred between systems over the Internet. Regardless of each machine's platform or operating system, if the same Internet Protocol is used by each machine then they will be able to transfer data to each other. The term "IP" is also commonly used as a further abbreviation of the term "IP Address". The current standard Internet Protocol is IP version 4 (IPv4).

Internet Protocol is addressed in RFC-791, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc791.txt
```

IP Address—Occasionally called an IP Number, IP Address stands for **I**nternet **P**rotocol Address and is used to identify a particular TCP/IP network and the hosts or machines on that network. It is a 32-bit numeric address containing four numbers between 0 and 255 separated by dots (e.g. "127.0.0.1"). Within an isolated network, each computer must have a unique IP address, which can be assigned at random. But, every computer on the Internet must have a registered IP address to avoid duplication. Each Internet IP address can be either static or dynamic. Static addresses do not change and always represent the same location or machine on the Internet. Dynamic IP addresses change and are usually assigned by an ISP to computers that are only on the Internet temporarily—such as when a user with a dial-up account accesses the Internet. However, it is still possible for a dial-up account to have a static IP address assigned to it.

ISPs and large organizations usually attempt to acquire a range or set of IP addresses from the InterNIC Registration Service so that all clients on their network or using their service may have similar addresses. These sets are broken up into three classes: Class A, B, and C. Class A and B sets are used by very large organizations and support 16 million and 65,000 hosts respectively. Class C sets are for smaller networks and support 255 hosts. Class A and B sets are now very difficult to get due to the shortage of available addresses; consequently most companies have to settle for multiple class C sets instead. Because of this IP address shortage, there is a new IP address protocol called Classless Inter-domain Routing (CIDR) that is gradually replacing the older system.

The current Internet Protocol standard, IPv4, is addressed in RFC-791, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc791.txt
```

IP version 6 (IPv6) is addressed in RFC-2460 at:

```
http://www.rfc-editor.org/rfc/rfc2460.txt
```

CIDR is addressed in RFCs 1517-1519 at:

```
http://www.rfc-editor.org/rfc/rfc1517.txt
http://www.rfc-editor.org/rfc/rfc1518.txt
http://www.rfc-editor.org/rfc/rfc1519.txt
```

IP Number—See *IP Address* above.

ISP—An **I**nternet **S**ervice **P**rovider (ISP) is a company that provides Internet access and services to the end user. Most ISPs provide multiple Internet services to their customers, such as: WWW access, email, access to newsgroups and news servers, and so on. Typically, users will connect to their ISP via dial-up, or some other form of connection, and then the ISP will connect them to a router, which will in turn route them to the Internet backbone.

Java—Developed by Sun Microsystems, Java is a network-oriented computer programming language with syntax much like C/C++ but is structured around classes instead of functions. In Internet applications it is commonly used for programming applets, which are small programs embedded in web pages. These programs can be automatically downloaded and executed by a user's browser in order to provide a large number of functions that wouldn't ordinarily be possible with just HTML or other scripting languages, and without fear of viruses or harm to your computer. Because Java is both efficient and easy to use, it is becoming popular among many software and hardware developers.

JavaScript—Not to be confused with Java, JavaScript was developed by Netscape as a scripting language designed to extend the capabilities of HTML and create interactive web pages. It is a highly pared down and easy to use programming language, which makes it much easier to use than Java and other languages but also limits it to some degree. It spite of its limitations it is very useful for adding a number if interactive elements to web sites. For example, JavaScript is useful when you want data to be preprocessed before it is submitted to the server, or when you want your pages to respond to user interaction with links or form elements. It can also be used to control plug-ins and applets based on user choices, and to accomplish a large number of other functions. JavaScript is included within the text of HTML documents and is interpreted by web browsers in order to perform the functions.

JPEG—A graphics file format that is very efficient at compressing high-color and photographic images—much more so than the GIF format. While GIF is the best choice for images containing regular shapes and large areas of repeating color patterns, JPEG is much more suited to images with irregular patterns and large numbers of colors. JPEG is the most commonly used format for high-color and photographic images on the Internet. The acronym JPEG stands for "**J**oint **P**hotographic **E**xperts **G**roup"—the group that developed the format.

Kbps—Commonly used when referring to modem speeds (e.g. 56 Kbps), this acronym stands for "**K**ilo**b**its **P**er **S**econd". It is the number of kilobits (1000 bits) of data being moved or processed every second. Note that this is kilo*bits* not kilo*bytes*—a kilobyte would be eight times more data than a kilobit.

Kilobyte—A kilobyte (K or KB) is a thousand bytes of computer data. Technically it is 1024 bytes (2^10 = 1024) but in normal usage it is usually rounded off to 1000 for simplicity.

LAN—A **L**ocal **A**rea **N**etwork (LAN) is a computer network limited to a single building or area, usually having all nodes (computers or workstations) connected together with some configuration of wires or cables or some other form of media. Most large companies have a LAN, which greatly simplifies the management and sharing of information amongst employees and offices. Most LANs utilize some form of email or chat system, and share devices such as printers in order to avoid having to have a separate device for each station. When the network's nodes are connected together via phone lines, radio waves, or satellite links it is called a Wide Area Network (WAN) instead of LAN.

Latency—The time it takes a data packet to move across a network connection. While a data packet is being sent, there is "latent" time during which the sending computer waits for a confirmation that the packet has been received. In addition to bandwidth, latency is one of the factors that determine the speed of your connection.

LDAP—Lightweight **D**irectory **A**ccess **P**rotocol (LDAP) is an online directory service protocol that is a simplification of Directory Access Protocol (DAP). The directory system is in a hierarchical structure consisting of the following levels: The "root" or starting directory, country, organization, organizational unit, and individual within that unit. Each LDAP entry is a collection of attributes with a unique identifier, called a distinguished name (DN). Because it is an open protocol, is efficient, and has the ability to be distributed across many servers, LDAP may eventually make it possible for virtually any application on any platform to access directory information for locating email addresses, organizations, files, and so on worldwide.

LDAP is addressed in RFC-2251, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2251.txt
```

Link—See *Hyperlink* above.

List server—A server application that is used to distribute email messages to multiple recipients by simply addressing the message to a single address. Simply put, when an email message is addressed to a *mailing list* maintained by the list server it will be automatically broadcast to the members of the list. Mailing lists typically have a single normal email address (for example, listname@example.com) but that address refers to a whole list of recipients rather than to a specific person or mailbox. When someone *subscribes* to a mailing list, the list server will automatically add the address to the list and distribute future emails directed to the list to that address, or member, and all other members. When someone unsubscribes, the list server simply removes the address so that it will receive no further list messages.

Frequently the term listserv is used generically to refer to any mailing list server. However, Listserv® is a registered trademark of L-Soft international, Inc. and is a specific program developed by Eric Thomas for BITNET in 1986. Besides other list servers, Alt-N Technologies' MDaemon server is equipped with an entire suite of list server, or mailing list, functions and features.

Logon—a unique code or series of characters used to gain access or otherwise identify yourself to a server or machine. In most cases a password must accompany the logon in order to gain access.

There are many terms used synonymously with "logon", such as *login*, *username*, *user name*, *user ID*, *sign-in*, and others. Frequently, "logon" is also used as a verb. For example, "I am going to *logon* to the mail server". In that context, however, the more common usage (and perhaps more proper) is "I am going to *log on* to the mail server".

Mailbox—An area in memory or on a storage device that is assigned to a specific email address and where email messages are stored. In any email system, each user has a private mailbox in which messages are stored when that user's mail server receives them. It is also common for the term "mailbox" to be used when referring to the leftmost portion of an email address. For example, "Frank" in "Frank@altn.com" is the mailbox while "altn.com" is the domain name.

Mailing List—Also called email groups, a mailing list is a list or group of email addresses identified by a single email address. For example, "listname@example.com". Typically when a list server receives an email message addressed to one of its mailing lists that message will be automatically distributed to all of the list's members (i.e. the addresses included in the list). Alt-N Technologies' MDaemon server is equipped with an extensive suite of mailing list features that enable lists to be public or private (anyone can post or join, or only members can post or join), moderated (each message must be approved by someone before it will go to the list), sent in digest format or as individual messages, and used in a variety of other ways.

Megabyte—Though technically 1,048,576 bytes (or 1024 kilobytes), a megabyte is more commonly rounded off and used to refer to a million bytes. Megabyte is abbreviated: "MB", as in "20 MB".

MIME—Defined in 1992 by the Internet Engineering Task Force (IETF), **M**ultipurpose **I**nternet **M**ail **E**xtensions (MIME) is the standard encoding method used for attaching non-text files to standard Internet email messages. Because typically only plain text files can be transferred via email, non-text files must first be encoding into a plain text format and then decoded after reaching their destination. Thus, an email program is said to be MIME Compliant if it can both send and receive files using the MIME standard. When a MIME-encoded message attachment is sent, generally both the type of file being sent and the method that should be used to turn it back into its original form are specified as part of the message. There are many predefined MIME content types, such as "image/jpeg" and "text/plain". However, it is also possible to define your own MIME types.

The MIME standard is also used by web servers to identify the files they are sending to web browsers. Because web browsers support various MIME types, this enables the browser to display or output files that are not in HTML format. Further, by updating the browser's lists of MIME-Types and the software used for handling each type, new file formats can be readily supported.

MIME is addressed in RFCs 2045-2049, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2045.txt
http://www.rfc-editor.org/rfc/rfc2046.txt
http://www.rfc-editor.org/rfc/rfc2047.txt
http://www.rfc-editor.org/rfc/rfc2048.txt
http://www.rfc-editor.org/rfc/rfc2049.txt
```

Mirror—A server (usually an FTP server) that has a copy of the same files that are on another server. Its purpose is generally to provide an alternate location from which the mirrored files can be downloaded should the original server go down or be overloaded. The term "mirror" can also refer to a configuration whereby information is written to more than one hard disk simultaneously. This is used as a redundancy measure so that if one disk fails the computer can continue to operate without losing any vital data.

Modem—An acronym derived from **mo**dulator-**dem**odulator. A modem is a device connected to a computer that enables the transfer of data to other computers over telephone lines. The modem converts the computer's digital data to an analog format (modulates) and then transmits it to another modem where the process is reversed (demodulates). Put simply, a modem is an analog-to-digital and digital-to-analog converter. The speed at which the data is transferred is expressed in either baud-rate (e.g. 9600 baud) or kilobits per second (e.g. 28.8 kbps).

MultiPOP—A component of Alt-N Technologies' MDaemon email server that can be configured to collect email, via the POP3 protocol, simultaneously from various email servers on behalf of MDaemon's users. This makes it possible for MDaemon account holders who have email accounts elsewhere on other email servers to have that email collected and pooled with their MDaemon account email. Thus storing all of their email in a single mailbox.

NAT—See Network Address Translation below.

Network—Two or more computers connected together in some fashion. The purpose of a network is to enable the sharing of resources and information between multiple systems. Some common examples are: multiple computers sharing printers, DVD-ROM drives, hard disks, individual files, and so on.

There are many types of networks, but the most broadly defined types are Local Area Networks (LANs) and Wide Area Networks (WANs). In a LAN, the individual computers (or nodes) are geographically close together—usually in the same building. They are also usually connected together directly with wires, although wireless connections are becoming common as well. The nodes in a WAN are usually farther apart (in another building or city) and connected via telephone lines, satellite hook-up, or some other form of connection.

The Internet itself is a network. It is often described as a network of networks.

Network Address Translation—Network address translation (NAT) is a system whereby two sets of Internet Protocol addresses (IP addresses) are used by a single network—one for external traffic and the other for internal traffic. This is mainly used as a firewall measure to help ensure network security. Your computer will appear to have a certain IP address to computers outside your LAN while your actual IP address is altogether different. Hardware or software placed "between" your network and the Internet performs the translations between the two addresses. Using this method, it is common for multiple computers in a LAN to "share" one company IP address. Thus there is no way for someone outside your network to know your actual address and directly connect to your computer without it first being qualified or authenticated during the translation.

Network Interface Card—A network interface card (NIC) is a computer circuit board that enables a computer to be connected to a network. NICs provide a full-time network connection whereas a modem (used by most home computers to dial-in to a network via telephone lines) usually provides only a temporary connection. Most NICs are designed for specific types of networks and protocols, such as Ethernet or token ring and TCP/IP.

Network News Transfer Protocol—See NNTP below.

NIC—See Network Interface Card above.

NNTP—Network **N**ews **T**ransfer **P**rotocol (NNTP) is the protocol used to transfer and distribute messages on USENET newsgroups. The most common and popular browsers and email clients now have NNTP clients built-in.

NNTP is addressed in RFC-977, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc977.txt
```

Node—Any single computer connected to a network.

ODMR—On-**D**emand **M**ail **R**elay is a new protocol designed to enable mail servers with only an intermittent connection to a service provider, and which do not have a static IP address, to receive mail similarly to those servers that do have one and use the `ETRN` command. If the system has a static IP address, the ESMTP ETRN command can be used. However, systems with dynamic IP addresses have no widely deployed solution. ODMR solves this problem. Among other things, ODMR introduces the Authenticated TURN command (`ATRN`) which causes the flow of an SMTP session to be reversed (like the older TURN command) but with the added security of requiring that the requesting server be authenticated. This makes it possible for an SMTP server with a dynamic IP address to connect to its ISP and have one or more host's email delivered to it via SMTP rather than collect it via POP or IMAP. This helps meet the widespread demand for a low-cost solution for those companies that need to their own mail server but cannot afford a static IP address or dedicated online presence.

ODMR is addressed in RFC 2645, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc2645.txt
```

OEM—Original **E**quipment **M**anufacturer (OEM) is an often confusing and misunderstood term. An OEM is a company that uses another company's equipment or products in its own product that is packaged and sold under a different brand or company name. For example, HyperMegaGlobalCom, Inc. is an OEM because it purchases computer components from one or more different companies, puts them all together into a single customized product, and then sells it with "HyperMegaGlobalCom" stamped on it. The company that sold HyperMegaGlobalCom the components might also be an OEM if they in turn got their components from someone else as well. "OEM" is an unfortunate misnomer because OEMs are not actually the original manufacturers; they are the "packagers" or "customizers". In spite of this, many people still often use the term "OEM" when referring to the actual hardware manufacturers instead of those who repackage it—and understandably so.

On the fly—The term "on the fly" is commonly used it two different ways. First, it is often used to denote something that can be done "in a hurry" or easily while "in the middle" of performing some other task. For example, a bookkeeping product might support creating accounts "on the fly" while in the middle of entering sales figures—"Simply stop entering figures, click button X, enter a name, and then continue entering more figures." The other way that "on the fly" is used is in referring to something that can be generated dynamically or automatically instead of manually or statically. For example, by using the information stored in a "cookie" a customized web page might be generated "on the fly" when a user returns to a web site. Rather than requiring someone to manually create a page customized to the user's tastes, it would be generated dynamically based upon that person's actions while browsing.

Original Equipment Manufacturer—See OEM above.

Packet—A unit of computer data sent over a network. Any time you receive data from another computer on your LAN or over the Internet it comes to your computer in the form of "packets". The original file or message is divided into these packets, transmitted, and then recombined at the destination. Each packet contains a header containing its source and destination, a block of data content, and an error-checking code. It is also "numbered" so that it can be connected to related packets being sent. The process of sending and receiving packets is known as "packet-switching". Packets are also commonly called "datagrams".

Packet Switching—The process of sending and receiving packets over a network or the Internet. In contrast to circuit switching (such as in an analog telephone), which sends the data in a continuous stream over a single path or circuit, packet switching transmits the data broken up into "packets", which may not necessarily take the same route to get to their destination. Further, because the data is in separate units, multiple users can send different files simultaneously over the same path.

Parameter—A parameter is a characteristic or value. In computing, it is any value passed to a program by a user or another program. Your name and password, a preference setting, font size, and so on are all parameters. In programming, a parameter is a value that is passed to a subroutine or function for processing.

PDF—Portable **D**ocument **F**ormat (PDF) is a highly compressed multi-platform file format developed by Adobe Systems Incorporated that captures document formatting, text, and images from a variety of applications. This makes it possible for the document to appear the same and print accurately on multiple computers and platforms (unlike many word processors). Viewing a PDF file requires the Adobe Acrobat Reader, a free application distributed by Adobe Systems. There is also a plug-in for viewing PDF files with your web browser. This makes it possible to view PDF files posted on a web site directly instead of having to download them first and then view them with a separate program.

Parse—In linguistics, to parse is to divide language into its grammatical components that can be analyzed. For example, dividing a sentence into verbs, adjectives, nouns, and so on.

In computers, to parse is to divide a computer language statement into parts that can be made useful for the computer. A parser in a compiler is takes each program statement that a developer has written and divides it into parts that can then be used for developing further actions or for creating the instructions that form an executable program.

Alt-N Technologies' MDaemon server and other products often parse email messages to determine their destination or to process them through filters and other tools.

Ping—An acronym for **P**acket **In**ternet **G**roper. It is a basic Internet program used to determine whether a specific IP address is reachable and accepting requests. It does this by sending an Internet Control Message Protocol (ICMP) Echo request and waiting for a response. "Ping" is commonly used as a verb when referring to this process. For example, "I am going to ping that server to see if it is online." "Pinging" an IP address is usually as simple as typing "ping" followed by the IP address or domain at the DOS prompt. For example "Ping 1.2.3.4."

ICMP is addressed in RFC-792 and the Echo protocol is addressed in RFC-862. These can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc792.txt
http://www.rfc-editor.org/rfc/rfc862.txt
```

POP—Stands for **P**ost **O**ffice **P**rotocol. POP (also commonly appears as POP3) is the most commonly used email protocol for retrieving email from a mail server. Most email clients use the POP protocol although some also support the newer IMAP protocol as well. POP2 became a standard in the mid 1980s and required SMTP to send messages. It was replaced by the newer version, POP3, which can be used with or without SMTP. POP is sometimes used as a verb when referring to collecting your email from a server. For example, "I'm going to POP my mailbox to get my mail."

POP3 is addressed in RFC-1939, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc1939.txt
```

Port—In TCP/IP and UDP networks and the Internet, a port is the endpoint of a logical connection and is identified by a number from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged protocols and services. For example, web servers typically are listed on port 80, SMTP servers typically communicate on port 25, and POP servers send and receive mail on 25. Generally, only one program at a time can use, or "bind", to any given port on each machine. When browsing the Internet, oftentimes certain servers will be running on non-default ports, which require you to specify the port in the URL after a colon. For example, "www.example.com:3000."

Port can also be used to refer to the sockets on a computer used for connecting peripheral devices and hardware to it. For example, serial ports, parallel ports, USB ports, and so on.

Finally, port is often used to describe the process of making a program designed for a specific platform or machine function on another platform. For example, "to port a Windows application to UNIX" or "to create a UNIX port for an application."

Post—In Internet messaging, such as email or newsgroups, it is a single message entered into a network communications system for others to see. For example, a message displayed on a newsgroup, mailing list, or discussion board is a post. It can also be used as a verb, as in "post a message to the mailing list or on the newsgroup."

PPP—Stands for "Point to Point Protocol." It is the Internet standard for dial-up connections. PPP is a set of rules that defines how your modem connection exchanges packets of data with other systems on the Internet.

PPP is addressed in RFC-1661, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc1661.txt
```

Protocol—In computing, a protocol is a set of guidelines or standards by which servers and applications communicate. There are many different protocols used for many different purposes, for example, TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP, and so on.

Registry—A database used by Microsoft Windows to store configuration information about software installed on the computer. This includes things like user settings, file extension associations, desktop background, color schemes, and many others. It has the following six parts:

HKEY_User—Stores user information for each user of the system.

HKEY_Current_User—Preferences for the current user.

HKEY_Current_Configuration—Stores settings for the display and printers.

HKEY_Classes_Root—File associations and OLE information.

HKEY_Local_Machine—Hardware, operating system, and installed application settings.

HKEY_Dyn_Data—Performance data.

When programs are installed on your computer the installer usually writes some information to the registry automatically. You can manually edit the registry, however, by using the regedit.exe program that is built in to Windows. But, you should exercise extreme caution when doing this because altering the wrong setting in the registry could cause your computer to function improperly, or not at all.

RFC—Request **F**or **C**omments is the name of the result and the process for creating a standard on the Internet. Each new standard and protocol is proposed and published on the Internet as a "Request For Comments". The Internet Engineering Task Force facilitates discussions on the new standard and eventually it is established. In spite of the fact that the standard is established and no further "comments" are "requested", the standard still retains the "Request for Comment" acronym along with its identifying number. For example RFC-822 is the official standard, or RFC, for email. However, those protocols that are officially adopted as "standards" do have an official standard number associated with them that is listed in the Internet Official Protocol Standards document (which itself is STD-1 and currently RFC-2900). You can find RFCs on the Internet at many locations but the authoritative source is The RFC Editor, located at `http://www.rfc-editor.org/`.

The Internet Official Protocol Standards document is located at:

```
http://www.rfc-editor.org/rfc/std/std1.txt
```

RTF—Rich **T**ext **F**ormat is a universal file format developed by Microsoft that is supported by nearly all word processors. In contrast to plain text format, RTF enables you to retain formatting, font information, text color, and so on. The file size of RTF files can be very large when compared to other file formats such as Word 2000's document format (*.doc) and Adobe PDF.

Server—A computer, or program, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as an SMTP server, or a machine on which the software is running. A single server *machine* could have many different server *programs* running on it concurrently. For example, your network's server might be running a web server, email server, FTP server, fax server, and others all at once.

SMTP—An acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is the primary protocol used to send email on the Internet from one server to another or from a client to a server. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Once a server has received email via SMTP it is usually stored there and can then be retrieved by a client via the POP, IMAP, or other protocol.

The SMTP protocol is addressed in RFC-821, which can be viewed at:

```
http://www.rfc-editor.org/rfc/rfc821.txt
```

Spam—Junk mail on the Internet. "Spam" is most commonly used to refer to unsolicited bulk email, although it is often used to refer to any unwanted email in general. A "spammer" will obtain hundreds, thousands, or even hundreds of thousands of email addresses from various sources and then "spam" the list with a message or solicitation. "Spam" can, however, be used to refer to a newsgroup or discussion board posting as well, when the posting is some unwanted or unrelated advertisement for a product or web site.

Spam is quickly becoming a serious problem on the Internet, tying up a great deal of time and server resources. And because spammers oftentimes use various techniques to attempt to mask the origin of the message—such as "spoofing" their addresses to appear to be someone else or attempting to relay the spam covertly through multiple mail servers—preventing it can be a challenge. Alt-N Technologies' MDaemon server is equipped with a number of features designed specifically to aid in fighting spam, such as: Spam Blocker, IP Shielding, IP Screening, Relay Control, and others.

The origin of using the term "Spam" to refer to junk email is debated, but it is generally accepted that it comes from a popular Monty Python sketch in which the word "spam" is repeated over and over and periodically accompanied by Vikings singing, "Spam spam spam spam, spam spam spam spam…" However, it may simply be a disparaging comparison to the trademarked Hormel meat product of the same name—everybody gets it at one time or another, but does anyone ever really ask for it or like it?

TCP/IP—Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (TCP/IP) has been described as the foundation of the Internet. It is the basic suite of communication protocols used on the Internet to connect hosts. It is the most commonly used protocol on Local Area Networks as well. It is a two-layer system, the topmost layer being TCP, which manages the disassembling and assembling of files into packets for transmitting over the network. IP, which is the lower layer, handles the addressing of the packets so that they get to the proper destinations. TCP is addressed in the following RFC-793. IP is addressed in RFC-791. These RFCs can be found at:

TCP – `http://www.rfc-editor.org/rfc/rfc793.txt`

IP – `http://www.rfc-editor.org/rfc/rfc791.txt`

Telnet—A command and program used to log on to Internet sites that support Telnet access. The Telnet command gets you to the logon prompt of the Telnet server. If you have an account on that server, you can access your permitted resources such as your files, email, and so on. The downside of Telnet is that it is a command line program that uses Unix commands.

The TELNET protocol is addressed in RFCs 854-855, which can be viewed at:

`http://www.rfc-editor.org/rfc/rfc854.txt`

`http://www.rfc-editor.org/rfc/rfc855.txt`

Terminal—A device that allows you to send commands to a remote computer. A terminal is a keyboard, display screen, and some simple circuitry. Oftentimes, however, personal computers are used to "emulate" terminals.

Tiff—An acronym for **T**agged **I**mage **F**ile **F**ormat. It is a graphics file format created to be a universal graphics translator across multiple computer platforms. TIFF can handle color depths ranging from 1-bit to 24-bit.

UDP—User **D**atagram **P**rotocol (UDP) is one of the protocols that make up the TCP/IP suite of protocols used for data transfers. UDP is a known as a stateless protocol because it doesn't acknowledge that packets being sent have been received.

UDP is addressed in RFC-768, which can be viewed at:

`http://www.rfc-editor.org/rfc/rfc768.txt`

Unix—Unix, or UNIX, is an operating system created by Bell Labs in the 1960s. Designed to be used by many users at the same time, it is the most popular operating system for servers on the Internet. There are now many different operating systems based on UNIX such as Linux, GNU, Ultrix, XENIX, and others.

URL—Every file or server on the Internet has a **U**niform **R**esource **L**ocator (URL). It is the address that you enter into your web browser to get to that server or file. URLs cannot have spaces and always use forward slashes. They have two parts separated by "://". The first part is the protocol being used or resource being addressed (for example, http, telnet, ftp, and so on) and the second part is the Internet address of the file or server (for example, www.altn.com or 127.0.0.1).

Uuencode—A set of algorithms for converting files into a series of 7-bit ASCII characters for transmission over the Internet. Although it stands for Unix-to-Unix encode, it is no longer exclusive to UNIX. It has become a universal protocol used to transfer files between different platforms. It is an encoding method commonly used in email.

WAN—A WAN, or **W**ide **A**rea **N**etwork, is similar to a Local Area Network (LAN) but is usually spread across multiple buildings, or even cities. WANs are sometimes composed of smaller LANs that are interconnected. The Internet could be described as the biggest WAN in the world.

Zip—Refers to a compressed or "zipped" file, usually with the "`.zip`" file extension. "Zipping" is compressing one or more files into a single archive file in order to save space for storage or to facilitate faster transfer to another computer. To use a zip file, however, you'll need to unzip it first with the appropriate program such as PKZIP or WinZip. There are multiple compression/decompression utilities available—both shareware and freeware—from many sites on the Internet. Hopefully you won't have to unzip the utility before you can install it.

Index